Guide du développeur

AWS Lambda

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Lambda: Guide du développeur

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Les marques commerciales et la présentation commerciale d'Amazon ne peuvent pas être utilisées en relation avec un produit ou un service extérieur à Amazon, d'une manière susceptible d'entraîner une confusion chez les clients, ou d'une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d'Amazon sont la propriété de leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

Table of Contents

Qu'est-ce que AWS Lambda? 1
Comparaison des primitives de calcul Lambda 2
Guide de configuration de l'agent 6
Conditions préalables 6
Claude Code 6
Installez le plugin aws-core depuis Agent Toolkit pour AWS 7
Codex 7
Installez le plugin aws-core depuis Agent Toolkit pour AWS 7
Curseur 7
Installation AWS compétence sans serveur 7
Kiro 7
Installation AWS compétence sans serveur dans la CLI Kiro 7
Installer les pouvoirs Kiro (depuis Kiro IDE) 7
GitHub Copilote 8
Installation AWS compétence sans serveur 8
Ordinateur de bureau Devin 8
Installation AWS compétence sans serveur 8
OpenCode 8
Installation AWS compétence sans serveur 8
Pour tous les autres agents compatibles avec les compétences des agents 8
Installation AWS compétence sans serveur 8
Installer des compétences Lambda supplémentaires 9
Fonctions événementielles 11
Quand utiliser les fonctions événementielles 11
Fonctions événementielles et fonctions durables 12
Fonctionnement de Lambda 13
Fonctionnalités principales 13
Informations connexes 14
Concepts de base 15
Fonctions Lambda et gestionnaires de fonctions 15
Environnement d’exécution et exécutions Lambda 16
Événements et déclencheurs 17
Autorisations et rôles Lambda 18
Exécution du code 20

Création d'architectures guidées par les événements 36
Conception d'une application 49
Création de votre première fonction 57
Inscrivez-vous pour Compte AWS 57
Créer la fonction 57
Invoquer la fonction 64
Nettoyage 68
Étapes suivantes 69
Exemples d'applications et de modèles 70
Traitement des fichiers 70
Intégration de base de données 70
Tâches planifiées 71
Ressources supplémentaires 71
File-processing appli 72
Scheduled-maintenance appli 97
Langages de programmation 117
Construire avec Node.js 118
Construire avec TypeScript 199
Création avec Python 250
Création avec Ruby 352
Création avec Java 422
Création avec Go 538
Création avec C# 600
Construire avec PowerShell 690
Création avec Rust 705
Runtimes 731
Environnements d'exécution pris en charge 732
Nouvelles versions d'exécution 736
politique d'obsolescence de l'exécution 737
Modèle de responsabilité partagée 738
Environnement d'exécution utilisé après la date d'obsolescence 740
Réception de notifications d'obsolescence lors de l'exécution 742
Environnements d'exécution obsolètes 743
Mises à jour de version de l'environnement d'exécution 747
Obtenir des données sur les fonctions par environnement d'exécution 761
Modifications de l'environnement d'exécution 768

API de runtime 772
OS-only runtimes 782
Référentiels open source 798
Configuration des fonctions événementielles 801
Archives de fichiers .zip 804
Images de conteneurs 818
Self-managed Stockage de code S3 828
Mémoire 834
Stockage éphémère 838
Kits d'instructions (ARM/x86) 841
Timeout 845
Variables d’environnement 848
Attachement de fonctions à un VPC 862
Attachement de fonctions aux ressources d’un autre compte 879
Accès Internet pour les fonctions VPC 886
Réseaux entrants 912
Systèmes de fichiers 917
les alias ; 926
Versions 934
Étiquettes 939
Streaming des réponses 944
Point final de métadonnées 956
Invocation de fonctions d'événement 961
Invocation synchrone 963
invocation asynchrone 967
Mappages de source d’événement 982
Filtrage des événements 995
Test dans la console 1012
États des fonctions 1016
Nouvelles tentatives 1020
Détection de boucle récursive 1022
URL de fonctions 1032
Dimensionnement des fonctions d'événement 1086
Comprendre et visualiser la simultanéité 1087
Calcul de la simultanéité pour une fonction événementielle 1091
Présentation de la simultanéité réservée et de la simultanéité allouée 1093

Présentation de la simultanéité et des requêtes par seconde 1103
Quotas de simultanéité 1105
Configuration de la simultanéité réservée 1107
Configuration de la simultanéité provisionnée 1112
Comportement de mise à l'échelle 1124
Surveillance de la simultanéité 1126
Surveillance et débogage 1132
Tarification 1133
Métriques des fonctions événementielles 1134
Journaux des fonctions d'événements 1147
CloudTrail journaux 1191
AWS X-Ray 1200
Informations sur les fonctions événementielles 1209
Affichage des métriques d'application 1218
Vigie applicative 1221
Déboguer avec VS Code 1225
Intégration d'autres services 1228
Création d'un déclencheur 1229
Liste des services 1230
Apache Kafka 1232
API Gateway 1405
Compositeur d'infrastructure 1437
CloudFormation 1441
Amazon DocumentDB 1444
DynamoDB 1484
EC2 1549
Elastic Load Balancing (Application Load Balancer) 1551
Invoquer à l'aide d'un EventBridge planificateur 1555
IoT 1558
Kinesis Data Streams 1560
Kubernetes 1623
MQ 1626
RDS 1649
S3 1681
Secrets Manager 1737
SQS 1757

Step Functions 1820
Lot S3 1831
SNS 1834
Fonctions durables 1856
Principaux avantages 1857
Quand utiliser des fonctions durables 1857
Comment ça marche 1859
Étapes suivantes 1860
Concepts de base 1861
Création de fonctions durables 1865
Configuration de fonctions durables 1894
Fonctions durables ou Step Functions 1896
Exemples 1899
Sécurité et autorisations 1925
Chiffrement des données d'exécution durables 1932
SDK d'exécution durable 1948
Invoquer des fonctions durables 1959
Tester des fonctions durables 1983
Surveillance des fonctions durables 1984
Bonnes pratiques 1990
SnapStart 1992
Cas d’utilisation 1993
Fonctions prises en charge et limitations 1994
Régions prises en charge 1995
Considérations de compatibilité 1995
Tarification 1996
Activation SnapStart 1997
Gestion de l’unicité 2004
Hooks d’exécution 2011
Contrôle 2026
Modèle de sécurité 2029
Bonnes pratiques 2030
Résolution des problèmes 2036
Isolement des locataires 2039
Quand utiliser le mode d'isolation des locataires 2040
Fonctions prises en charge et limitations 2041

Pris en charge Régions AWS 2041
Considérations 2041
Tarification 2041
Mode d'isolation 2042
Permettre l'isolement des locataires 2043
Invocation de fonctions avec isolation des locataires 2046
Accès en code 2051
Contrôle 2055
Résolution des problèmes 2057
Instances gérées 2058
Fonctionnalités clés 2058
Quand utiliser les instances gérées Lambda 2058
Comment ça marche 2059
Modèle de simultanéité 2059
Location et isolement 2060
Tarification 2060
Différences entre les instances gérées Lambda et le type de calcul Lambda (par défaut) .. 2061
Étapes suivantes 2062
Prise en main 2063
Concepts de base 2070
Déploiements 2097
Runtimes 2106
Mise en réseau 2132
Contrôle 2136
Quotas 2153
Bonnes pratiques 2156
Résolution des problèmes 2161
Layers 2171
Utilisation des couches 2174
Couches et versions de couches 2174
Empaquetage des couches 2176
Création et suppression de couches 2180
Ajout de couches 2184
Couches avec CloudFormation 2188
Couches avec AWS SAM 2189
Extensions 2189

Environnement d’exécution 2191
Impact sur les performances et les ressources 2192
Permissions 2193
Configuration des extensions 2194
Partenaires des extensions 2196
API d’extensions 2198
API de télémétrie 2216
Résolution des problèmes 2273
Configuration 2274
Déploiement 2284
Invocation 2291
Exécution 2300
Mappage des sources d’événements 2311
Réseaux 2316
Bonnes pratiques 2319
Code de fonction de l'événement 2319
Configuration de la fonction d'événement 2321
Extensibilité des fonctions événementielles 2322
Métriques et alarmes 2323
Utilisation des flux 2324
Bonnes pratiques de sécurité 2325
Exemples d’applications 2326
Outils de développement 2329
Outils de développement locaux 2330
Outils d’infrastructure en tant que code (IaC) 2330
GitHub Outils d'actions 2331
Outils électriques pour AWS Lambda 2331
Outils de gestion des flux de travail et des événements 2332
Développement local 2332
GitHub Actions 2341
Infrastructure en tant que code (IaC) 2342
Outils électriques pour Lambda AWS 2366
Flux de travail et événements 2368
Tests 2371
Résultats commerciaux ciblés 2372
Que faut-il tester ? 2373

Comment tester le sans serveur 2374
Techniques de test 2374
Bonnes pratiques 2381
Défis liés aux tests locaux 2385
FAQ 2387
Prochaines étapes et ressources 2388
Permissions 2389
Rôle d'exécution (autorisations pour les fonctions d'accéder à d'autres ressources) 2392
Autorisations d'accès (autorisations permettant à d'autres entités d'accéder à vos fonctions) 2405
Fonctions Web 2450
Quand utiliser les fonctions Web 2451
Fonctionnement des fonctions Web 2452
Principaux avantages 2452
Concepts de base 2453
Modèle de ressources 2453
États de révision 2455
États de point de terminaison 2456
Environnements d'exécution 2458
Traitement des demandes 2459
Révisions 2460
Points de terminaison 2471
Créez votre première fonction Web 2477
Conditions préalables 2478
Création d'une fonction Web (console) 2479
Création d'une fonction Web (AWS CLI) 2481
Nettoyage 2486
Déploiement 2486
Code dans Amazon S3 2486
Modèles de déploiement 2492
Multi-Region déploiement 2501
Comportement HTTP 2506
Méthodes HTTP 2506
En-têtes de demandes 2506
En-têtes de réponse 2507
Limites d'en-têtes 2508

Mise en réseau 2508
Connectivité entrante 2509
Connectivité sortante 2512
Connexion d'une fonction Web à votre VPC 2513
Mettre à jour ou supprimer la connectivité VPC 2517
Prise en charge d’IPv6 2518
Mise à l’échelle 2519
Environnements d'exécution 2519
Limite de simultanéité dynamique par environnement 2520
Paramètres de dimensionnement 2521
Quotas de comptes 2523
Comment les paramètres de dimensionnement interagissent 2523
Étranglement 2525
Mise à l'échelle et réduction 2526
Choix des paramètres de dimensionnement 2526
Mise à l'échelle pour MultiRegion et PerRegion points finaux 2528
Exemples de dimensionnement 2528
Cycle de vie environnemental 2534
Phases du cycle de vie 2534
Initialisation (démarrage à froid) 2535
Scale-down et arrêt 2536
Réutilisation de l'environnement 2537
Gestion des demandes simultanées 2537
Runtimes 2538
Pris en charge Node.js versions 2538
Correctif automatique lors de l'exécution 2538
Frameworks Web pris en charge 2539
Node.js modèle d'exécution 2539
La mémoire et le Node.js tas 2540
Comment Lambda achemine les demandes vers votre application 2541
Configuration des fonctions Web 2542
Package de déploiement 2542
Architecture 2543
Timeout 2543
Variables d’environnement 2544
Étiquettes 2546

Point final de métadonnées 2547
Permissions 2549
Rôle d'exécution 2550
Resource-based politiques 2553
Autorisations pour configurer le réseau 2560
Contrôle d’accès 2561
Utilisation du type `IamAuth`d'authentification 2562
Utilisation du type `ApplicationManaged`d'authentification 2566
Gouvernance et contrôle d’accès 2567
Chiffrement au repos 2569
Options de chiffrement au repos 2570
Chiffrer les données au repos à l'aide d'une clé gérée par le client 2570
Surveillance de l'interaction des fonctions Web avec AWS KMS 2581
Contrôle 2582
Facturation par télémétrie 2584
Considérations relatives à la télémétrie 2585
Métriques 2587
Journaux 2595
Métriques personnalisées 2615
CloudTrail journaux 2617
Exemples d’applications 2628
Minimale Express vigie 2628
Honneur API et fichiers statiques 2629
Server-sent événements 2630
Multi-Region itinéraire de vérification 2630
Package et déploiement d'un échantillon 2630
Bonnes pratiques 2631
Sécurisez tous les terminaux 2631
Conservez les artefacts de déploiement immuables 2632
Conception pour les demandes simultanées 2632
Assurez la prévisibilité du démarrage 2633
Définissez des limites à partir du comportement mesuré 2633
Déploiement avec vérification et annulation explicites 2634
Établissez une base de référence opérationnelle 2634
Fonctionnement MultiRegion et PerRegion terminaux en tant que systèmes distribués 2635
Tests 2635

Couches de test recommandées 2636
Exécutez le serveur HTTP localement 2636
Testez le package de déploiement 2637
Testez dans un environnement cloud isolé 2637
Autorisation des tests et exposition 2638
Testez la simultanéité, la mise à l'échelle et la régulation 2638
Tester les déploiements et les annulations 2639
Résolution des problèmes 2639
Collecter des informations de diagnostic 2639
Problèmes de déploiement et de démarrage 2640
Erreurs de CLI et de package 2642
Défaillances des requêtes HTTP 2644
Limites des en-têtes de demande 2647
Types d'erreur liés aux fonctions Web 2649
Des journaux ou des statistiques sont manquants 2652
Problèmes de stockage et de chiffrement du code 2653
Problèmes liés `MultiRegion`aux `PerRegion`terminaux 2653
Problèmes de réseau et de connectivité 2654
Préparer un bundle d'escalade 2656
Informations connexes 2656
MicroVM 2657
Comment fonctionnent les micromachines virtuelles Lambda 2657
Quand utiliser Lambda MicroVMS 2658
Fonctionnalités principales 2659
Concepts de base 2659
Concepts clés 2659
Comment Lambda construit votre image 2660
Cycle de vie de la microVM 2661
Créez votre première microVM 2663
Conditions préalables 2663
Création de votre première image microVM 2665
Exécution de votre première microVM 2667
Connexion à votre microVM 2668
Nettoyage 2669
Étapes suivantes 2669
Images microVM 2669

Comment Lambda crée une image microVM 2670
Dimensionnement des microVM 2670
Images de base MicroVM 2671
Hooks de création d'images MicroVM 2672
Mise à jour d'une image MicroVM 2674
États de l'image et états de construction 2675
Variables d’environnement 2676
Instantanés 2676
Correctifs d'images sur microVM 2678
Images de base de conteneur 2678
Fonctionnalités du système d'exploitation 2679
Exécution de microVMS 2680
Démarrage d'une microVM 2680
Connexion à une microVM 2683
Hooks de cycle de vie 2686
Suspension et reprise des microVM 2690
Mise à l'échelle et simultanéité 2691
Terminer une microVM 2692
Répertorier les microVM 2692
Gestion des erreurs 2692
Mise en réseau 2694
Vue d’ensemble 2694
Connectivité entrante 2694
Connectivité sortante 2698
Utilisation de connecteurs réseau de sortie 2698
Utilisation de microVM Lambda avec des points de terminaison VPC d'interface (AWS PrivateLink) 2701
Sécurité 2707
Rôles IAM 2707
Jetons d'authentification 2708
Jetons d'accès Shell 2708
Balisage de ressources 2708
Référence des autorisations IAM 2709
Formats ARN des ressources 2710
Exemple : Least-privilege politique pour un opérateur 2710
Contrôle 2711

Journalisation (CloudWatch journaux) 2711
CloudTrail journalisation 2712
Résolution des problèmes 2716
Accès au shell 2716
Résolution des problèmes 2717
Erreurs courantes (création d'images) 2718
Résolution des problèmes liés au connecteur réseau 2719
Bonnes pratiques 2721
Conception de l’application 2721
Performance 2721
Sécurité 2722
Optimisation des coûts 2722
Contrôle 2723
Intégrations 2723
Agents gérés par Claude 2723
Agents Cursor Cloud 2728
API OpenAI Agents 2734
Sécurité, gouvernance et conformité 2744
Protection des données 2745
Chiffrement en transit 2746
Chiffrement au repos 2747
Utilisation des rôles liés à un service 2752
Service-linked autorisations de rôle pour Lambda 2753
Création d'un rôle lié à un service pour Lambda 2754
Modification d'un rôle lié à un service pour Lambda 2754
Supprimer un rôle lié à un service pour Lambda 2754
Régions prises en charge pour les rôles liés aux services Lambda 2755
Gestion de l’identité et des accès 2756
Public ciblé 2757
Authentification par des identités 2758
Gestion de l’accès à l’aide de politiques 2759
Comment ? AWS Lambda fonctionne avec IAM 2761
Identity-based exemples de politiques 2767
AWS politiques gérées 2770
Résolution des problèmes 2782
Gouvernance 2784

Contrôles proactifs avec Guard ... 2787
Contrôles proactifs avec AWS Config ... 2791
Contrôles de détective avec AWS Config ... 2799
Signature de code ... 2804
Analyse du code ... 2807
Observabilité ... 2812
Validation de conformité ... 2821
Résilience ... 2821
Sécurité de l'infrastructure ... 2823
Sécurisation des charges de travail avec des points de terminaison publics ... 2823
Authentification et autorisation ... 2823
Protection des points de terminaison d'API ... 2824
Signature de code ... 2825
Validation de signature ... 2826
Création d'une configuration ... 2827
Permissions ... 2829
Balises de configuration de signature de code ... 2831
Travailler avec AWS SDK ... 2835
Exemples de code utilisant le SDK ... 2837
Principes de base ... 2840
Hello Lambda ... 2841
Principes de base ... 2850
Actions ... 2987
Scénarios ... 3127
Confirmation automatique des utilisateurs connus avec une fonction Lambda ... 3128
Migration automatique des utilisateurs connus avec une fonction Lambda ... 3169
Créez une API REST pour effectuer le suivi COVID-19 données ... 3192
Créer une API REST de bibliothèque de prêt ... 3193
Créer une application de messagerie ... 3194
Création d'une API REST avec intégration de fonctions proxy ... 3195
Création d'une application sans serveur pour gérer des photos ... 3204
Créer une application de chat WebSocket ... 3208
Créez une application pour analyser les commentaires des clients ... 3209
Création d'un tableau de bord de surveillance avec le nom de fonction comme variable ... 3215
Création de votre première fonction sans serveur ... 3225
Invoquer une fonction Lambda à partir d'un navigateur ... 3237

Transformation de données avec S3 Object Lambda 3238
Utiliser API Gateway pour invoquer une fonction Lambda 3239
Utiliser les fonctions Step Functions pour invoquer des fonctions Lambda 3241
Utilisent des événements planifiés pour invoquer une fonction Lambda 3242
Utilisation de l'API Neptune pour interroger des données de graphe 3244
Utilisation de variables de propriété dans les tableaux de bord de surveillance pour surveiller plusieurs fonctions sans serveur 3244
Rédaction de données d'activité personnalisées à l'aide d'une fonction Lambda après authentification de l'utilisateur Amazon Cognito 3254
Exemples sans serveur 3276
Connexion à une base de données Amazon RDS dans une fonction Lambda 3277
Invoquer une fonction Lambda à partir d'un déclencheur Kinesis 3296
Invocation d'une fonction Lambda à partir d'un déclencheur DynamoDB 3307
Invocation d'une fonction Lambda à partir d'un déclencheur Amazon DocumentDB 3316
Invocation d'une fonction Lambda à partir d'un déclencheur Amazon MSK 3328
Invoquer une fonction Lambda à partir d'un déclencheur Amazon S3 3338
Invocation d'une fonction lambda à partir d'un déclencheur Amazon SNS 3350
Invoquer une fonction Lambda à partir d'un déclencheur Amazon SQS 3359
Signalement des échecs d'articles par lots pour les fonctions Lambda à l'aide d'un déclencheur Kinesis 3368
Signalement des échecs d'articles par lots pour les fonctions Lambda à l'aide d'un déclencheur DynamoDB 3381
Signalement des échecs d'articles par lots pour les fonctions Lambda à l'aide d'un déclencheur Amazon SQS 3392
AWS contributions communautaires 3402
Création et test d'une application sans serveur 3402
Quotas Lambda 3405
calcul et stockage 3407
Configuration, déploiement et exécution de fonction 3408
Requêtes d'API Lambda 3412
Fonctions durables 3414
MicroVM 3416
calcul et stockage 3417
Images et versions 3418
Per-MicroVM débit 3418
limites de débit d'API 3419

Fonctions Web Lambda 3419
Quotas relatifs aux fonctions Web, à la révision et à l'environnement d'exécution 3420
Quotas de points de terminaison 3421
Quotas de comptes 3423
Contraintes du réseau 3423
Autres services 3424
Historique de la documentation 3425
Mises à jour antérieures 3460
..... mmmcdlxix

Qu'est-ce que AWS Lambda?

AWS Lambda est un service de calcul sans serveur. Avec Lambda, vous pouvez exécuter du code sans avoir à provisionner ni à gérer des serveurs. Lambda gère automatiquement l'infrastructure sous-jacente, y compris la maintenance des serveurs, le provisionnement des capacités, le dimensionnement et l'application de correctifs, afin que vous puissiez vous concentrer sur la logique de votre application.

Lambda fournit trois primitives de calcul, chacune conçue pour différents modèles de charge de travail :

- Fonctions d'événements Lambda : exécutez du code en réponse à des événements ou à des appels d'API sans gérer de serveurs. Vous écrivez une fonction de gestionnaire, vous la connectez à un déclencheur (API Gateway, Amazon S3, Amazon SQS et plus de 200 AWS autres services) EventBridge, et Lambda l'exécute. Chaque appel s'exécute indépendamment, sans état partagé, et s'adapte horizontalement à la demande. Lambda gère les environnements d'exécution, le dimensionnement, le routage et la tolérance aux pannes.
- Lambda Web Functions : exécutez des applications Web et des backends d'API en tant que serveurs HTTP. Votre Node.js code écoute sur un port et gère directement les requêtes HTTP, à l'aide de frameworks Web tels que ExpressHono, ou React Router sans adaptateurs. Chaque environnement d'exécution répond à plusieurs demandes simultanées. Lambda fournit un point de terminaison HTTPS, adapte votre application en fonction du trafic (y compris jusqu'à zéro) et peut la répliquer. Régions AWS
- Lambda MicroVMS : environnements informatiques isolés dotés d'un démarrage quasi instantané et d'une durée de vie totale allant jusqu'à 8 heures (y compris le temps de fonctionnement et le temps de suspension). Conçu pour les charges de travail nécessitant un environnement informatique dédié à chaque utilisateur ou à chaque tâche. Lambda gère l'isolation, la capacité et le réseau. Votre application utilise les API Lambda MicroVMS et les points de terminaison HTTPS pour connecter chacun user/job à son environnement informatique.

> **Note**
>
> Event Functions est le nom du type de fonction Lambda d'origine qui exécute votre code en réponse à des événements et à des appels d'API. Le nom distingue ce type de fonction des fonctions Web Lambda et des microVM Lambda, et la console Lambda l'appelle fonction d'événement. La ressource sous-jacente reste inchangée : les opérations

d'API (telles que `CreateFunction` et`Invoke`), les AWS SDK, la AWS CLI, le type de `AWS::Lambda::Function` ressource et les ARN continuent d'utiliser des fonctions. Vous n'avez donc pas besoin de modifier le code, les modèles d'infrastructure ou les autorisations IAM.

Pour de plus amples informations sur la tarification, veuillez consulter AWS Lambda Pricing (français non garanti).

Comparaison des primitives de calcul Lambda

Les fonctions d'événement Lambda, les fonctions Web Lambda et les microVM Lambda partagent une base commune sans serveur :

- Aucune gestion de serveur : AWS gère l'infrastructure sous-jacente, les correctifs d'instance et la capacité.
- Pay-per-use facturation — Aucun engagement initial. Vous ne payez que pour les ressources utilisées.
- Réseau géré : tous les trois fournissent un accès réseau entrant et sortant géré par des services.
- Virtualisation Firecracker : VM-level isolation entre les charges de travail.

Bien qu'ils partagent cette base, ils répondent à différents cas d'utilisation :

	Fonctions d'événement Lambda	Fonctions Web Lambda	MicroVM Lambda
Idéal pour	Request-response ou charges de travail basées sur des événements (API, traitement des données, automatisation)	Applications Web et backends d'API qui servent directement le trafic HTTP	Environnements persistants exécutant du code utilisateur ou AI-produced non fiable
Modèle de programmation	Gestionnaire de fonctions invoqué dans un environnement d'exécution pris en charge	Serveur HTTP qui écoute sur un port, à l'aide de frameworks Web standard	N'importe quelle application : exécutez vos propres fichiers binaires, écoutez les ports, utilisez

	Fonctions d'événement Lambda	Fonctions Web Lambda	MicroVM Lambda
			les fonctionnalités du système d'exploitation Linux
Durée	Jusqu'à 15 minutes par appel par défaut ; jusqu'à 90 minutes par appel asynchrone ou par appel de mappage des sources d'événements sur les instances gérées Lambda ; flux de travail en plusieurs étapes d'une durée maximale d'un an avec Lambda Durable Functions	Jusqu'à 15 minutes par requête HTTP (30 secondes par défaut)	Jusqu'à 8 heures par session ; suspension et reprise d'une session à l'autre
Environnement d'exécution	Service-provided environnements d'exécution des langues ; prise en charge des environnements d'exécution fournis par le client	Environnements d'exécution Service-provided Node.js	Customer-provided Images de microVM
Réseau entrant	Invocations directes ou intégrations de sources d'événements aux services AWS	Service-provided Point de terminaison HTTPS avec TLS ; routage optionnel basé sur la latence entre Régions AWS	Accès entrant à n'importe quel port à l'aide des protocoles OSI de couche 7

	Fonctions d'événement Lambda	Fonctions Web Lambda	MicroVM Lambda
Simultanéité	Une demande par environnement d'exécution à la fois par défaut ; plusieurs demandes simultanées par environnement d'exécution pour les instances gérées Lambda	Plusieurs demandes simultanées par environnement d'exécution	Plusieurs connexions simultanées par microVM
État de l'environnement	Les environnements d'exécution peuvent être réutilisés (démarrages à chaud), mais l'état peut ne pas persister entre les invocations	Les environnements d'exécution peuvent être réutilisés (démarrages à chaud), mais l'état peut ne pas persister entre les invocations	État de la mémoire et du disque préservé lors de la suspension ; restauré lors de la reprise
Dimensionnement	Automatique : Lambda crée et détruit des environnements d'exécution en réponse au trafic	Automatique : Lambda crée et détruit des environnements d'exécution en réponse au trafic, en redimensionnant jusqu'à zéro en cas d'inactivité	Developer-controlled — vous créez, suspendez, reprenez et résiliez des microVM via l'API
Cycle de vie	Entièrement géré par Lambda	Entièrement géré par Lambda	Developer-controlled; politiques d'inactivité facultatives pour la suspension et la reprise automatiques

	Fonctions d'événement Lambda	Fonctions Web Lambda	MicroVM Lambda
Tarification	Per-request + GB-seconds du temps d'exécution	Par demande, plus le temps processeur actif (facturé par incréments de 1 ms) et la mémoire pendant la durée de vie de chaque environnement d'exécution	Per-second de calcul en cours d'exécution + stockage de snapshots en cas de suspension

Guide de configuration de l'agent

Les agents de codage basés sur l'IA peuvent accélérer le développement sans serveur en fournissant une assistance intelligente pour l'échafaudage des applications, la configuration du déploiement, le débogage et la génération d'infrastructures sous forme de code. En configurant votre agent avec la bonne combinaison de plugins et de compétences, vous le dotez de l'expertise requise pour créer et gérer des applications sans serveur.

> **Travaillez avec votre agent de codage**
>
> Pour une référence rapide, vous pouvez placer ce lien directement dans le contexte de votre agent :
>
> ```
> https://docs.aws.amazon.com/lambda/latest/dg/samples/aws-lambda-agent-setup.md
> ```

Choisissez la méthode d'installation adaptée à votre environnement de développement.

Conditions préalables

Assurez-vous que les conditions préalables suivantes sont réunies pour installer le plugin aws-core :

- UV installé sur votre système.
- (Facultatif) Et Compte AWS avec les informations d'identification IAM configurées sur votre machine locale. Les informations d'identification sont requises pour les outils qui exécutent des appels d' AWS API et exécutent des scripts, mais pas pour rechercher de la documentation ou découvrir des compétences. Si vous n'avez pas configuré d'informations d'identification, consultez Configuration du serveur AWS MCP pour obtenir des instructions détaillées.

Claude Code

Installez le plugin aws-core, qui fait partie de l'Agent Toolkit for AWS, qui regroupe la configuration du serveur AWS MCP et un ensemble de compétences d'agent (y compris la compétence sans serveur). AWS

Installez le plugin aws-core depuis Agent Toolkit pour AWS

Exécutez la commande suivante pour installer le plugin :

```
/plugin marketplace add aws/agent-toolkit-for-aws
/plugin install aws-core@agent-toolkit-for-aws
```

Cela permet d'installer les compétences de l'agent, notamment la compétence AWS sans serveur, les crochets d'agent et la configuration du serveur AWS MCP en une seule étape.

Codex

Installez le plugin aws-core depuis Agent Toolkit pour AWS

Exécutez la commande suivante pour installer le plugin :

```
codex plugin marketplace add aws/agent-toolkit-for-aws
```

Lancez ensuite Codex et lancez `/plugins` pour parcourir et installer le plugin aws-core.

Curseur

Installation AWS compétence sans serveur

```
npx skills add https://github.com/aws/agent-toolkit-for-aws --skill aws-serverless --
yes --global
```

Kiro

Installation AWS compétence sans serveur dans la CLI Kiro

```
npx skills add https://github.com/aws/agent-toolkit-for-aws --skill aws-serverless --
yes --global
```

Installer les pouvoirs Kiro (depuis Kiro IDE)

Installez les pouvoirs Kiro suivants qui fournissent des contextes et des outils spécialisés aux agents Kiro à la demande :

- Modèle d'application sans serveur (SAM) : installation via Kiro Powers Link.
- Instances gérées Lambda : installation via Kiro Powers Link.

GitHub Copilote

Installation AWS compétence sans serveur

```
npx skills add https://github.com/aws/agent-toolkit-for-aws --skill aws-serverless --
yes --global
```

Ordinateur de bureau Devin

Installation AWS compétence sans serveur

```
npx skills add https://github.com/aws/agent-toolkit-for-aws --skill aws-serverless --
yes --global
```

OpenCode

Installation AWS compétence sans serveur

```
npx skills add https://github.com/aws/agent-toolkit-for-aws --skill aws-serverless --
yes --global
```

Pour tous les autres agents compatibles avec les compétences des agents

Pour tout autre agent prenant en charge le format open source de compétences d'agent, procédez comme suit :

Installation AWS compétence sans serveur

```
npx skills add https://github.com/aws/agent-toolkit-for-aws --skill aws-serverless --
yes --global
```

Installer des compétences Lambda supplémentaires

Le kit d'outils des agents AWS inclut des compétences spécialisées sans serveur qui permettent à vos agents d'IA de connaître les fonctionnalités de Lambda. Installez ces compétences à l'aide de n'importe quel agent tel que Claude Code, Cursor, Kiro CLI, GitHub Copilot, Codex, Devin Desktop OpenCode ou tout autre agent compatible avec le format de compétences d'agent open source pour permettre à votre agent de vous aider à créer, déployer et gérer des charges de travail à l'aide de Lambda Web Functions, Lambda MicroVM, Lambda Managed Instances et Lambda Durable Functions.

1. Compétence Lambda Web Functions — Les fonctions Web Lambda vous permettent d'exécuter des applications Web et des backends d'API en tant que serveurs HTTP, où votre Node.js code gère les requêtes directement à l'aide de frameworks tels queExpress, Fastify ou, Hono Lambda fournissant un point de terminaison HTTPS, un dimensionnement automatique (y compris jusqu'à zéro) et une réplication multirégionale.

   ```
   npx skills add https://github.com/aws/agent-toolkit-for-aws/tree/main/skills/
   specialized-skills/serverless-skills/aws-lambda-web-functions --yes --global
   ```

2. Compétence Lambda MicroVMS — Lambda MicroVMS est une primitive de calcul sans serveur qui assure l' VM-level isolation, des vitesses de lancement et de reprise quasi instantanées, ainsi que la préservation de l'état pour l'exécution d'utilisateurs ou de code dans des environnements d'exécution isolés et dynamiques. AI-generated

   ```
   npx skills add https://github.com/aws/agent-toolkit-for-aws/tree/main/skills/
   specialized-skills/serverless-skills/aws-lambda-microvms --yes --global
   ```

3. Compétence relative aux instances gérées Lambda : avec les instances gérées Lambda, vous pouvez exécuter des fonctions Lambda sur vos instances Amazon EC2 tout en préservant la simplicité opérationnelle de Lambda, en vous donnant accès à des configurations de calcul spécialisées et à un meilleur rapport coût-efficacité grâce aux avantages tarifaires d'Amazon EC2 sans avoir à gérer l'infrastructure.

   ```
   npx skills add https://github.com/aws/agent-toolkit-for-aws/tree/main/skills/
   specialized-skills/serverless-skills/aws-lambda-managed-instances --yes --global
   ```

4. Compétence en matière de fonctions durables Lambda : les fonctions durables de Lambda vous permettent de créer des applications durables et tolérantes aux pannes, capables de contrôler la progression, de récupérer automatiquement en cas de panne et de suspendre l'exécution pendant

un an au maximum lorsque vous attendez des tâches de longue durée, telles que des processus humains intégrés.

```
npx skills add https://github.com/aws/agent-toolkit-for-aws/tree/main/skills/
specialized-skills/serverless-skills/aws-lambda-durable-functions --yes --global
```

AWS Lambda Event Functions (anciennement fonctions Lambda)

> **Tip**
>
> Rejoignez des experts Serverless pour participer à des ateliers pratiques gratuits afin d'apprendre à créer des applications sans serveur selon les meilleures pratiques. Inscrivez-vous à des ateliers sans serveur gratuits sur le site Web AWS d'Experience.

AWS Lambda Event Functions, anciennement appelées fonctions Lambda, exécutent votre code en réponse à des événements provenant de sources telles qu'Amazon Simple Storage Service (Amazon S3), Amazon Simple Queue Service (Amazon SQS), EventBridge sans avoir à gérer de serveurs. Une fonction reçoit un événement, exécute votre gestionnaire et renvoie une réponse. Les fonctions augmentent ou diminuent automatiquement grâce à la tarification à l'utilisation. Consultez Création de votre première fonction pour démarrer. Pour plus d'informations sur les meilleures pratiques, les langages de programmation, l'isolation des locataires et les outils de développement et de déploiement, consultez les rubriques connexes ci-dessous.

> **Note**
>
> Event Functions est le nom du type de fonction Lambda d'origine, et la console Lambda l'appelle fonction d'événement. La ressource sous-jacente est inchangée : les opérations d'API (telles que `CreateFunction` et`Invoke`), les AWS SDK, la AWS CLI et le type de `AWS::Lambda::Function` ressource utilisent toujours des fonctions, vous n'avez donc pas besoin de modifier le code ou la configuration.

Pour de plus amples informations sur la tarification, veuillez consulter AWS Lambda Pricing (français non garanti).

Quand utiliser les fonctions événementielles

Vous pouvez utiliser les fonctions d'événement pour :

- Traitement des fichiers : traitez automatiquement les fichiers lorsqu'ils sont chargés sur Amazon Simple Storage Service. Consultez les exemples de traitement de fichiers pour plus de détails.
- Long-running flux de travail : créez des flux de travail dynamiques en plusieurs étapes pouvant s'exécuter pendant un an au maximum. Voir les fonctions Lambda durables pour plus de détails.
- Exemples d'opérations et d'intégration de bases de données : répondez aux modifications de base de données et automatisez les flux de données. Consultez les exemples de bases de données pour plus de détails.
- Tâches planifiées et périodiques : exécutez des opérations automatisées selon un calendrier régulier à l'aide de EventBridge. Consultez les exemples de tâches planifiées pour plus de détails.
- Traitement des flux : traitez les flux de données en temps réel à des fins d'analytique et de surveillance. Consultez Kinesis Data Streams pour plus de détails.
- Applications Web : gérez les demandes Web et d'API via Amazon API Gateway, Application Load Balancer ou les URL des fonctions Lambda. Par défaut, chaque environnement d'exécution traite une demande à la fois. Sur les instances gérées Lambda, un environnement d'exécution gère plusieurs demandes simultanément.
- Backends mobiles : créez des backends d'API sécurisés pour les applications mobiles et Web.
- Backends IoT : gérez les demandes d'API Web, mobiles, IoT et tierces. Consultez IoT pour plus de détails.

Pour traiter le trafic HTTP directement depuis un serveur Web standard, utilisez les fonctions Web Lambda. Pour plus d'informations, consultez Fonctions Web.

Fonctions événementielles et fonctions durables

Les fonctions Lambda s'exécutent jusqu'à 15 minutes par appel par défaut et sont idéales pour les tâches axées sur les événements, telles que le traitement des demandes d'API, la gestion des téléchargements de fichiers ou la réponse aux modifications de base de données. Sur les instances gérées Lambda, les fonctions peuvent s'exécuter pendant 90 minutes maximum pour les appels asynchrones et de mappage des sources d'événements (ESM). Les fonctions durables étendent ce modèle aux charges de travail qui doivent s'exécuter plus longtemps et résister aux interruptions. Ils vérifient automatiquement leur progression afin qu'ils reprennent de manière fiable après un échec, et ils peuvent fonctionner jusqu'à un an lorsqu'ils sont invoqués de manière asynchrone. Utilisez des fonctions durables lorsque vous avez besoin de flux de travail en plusieurs étapes, d'approbations humaines ou d'une coordination entre les services sur de longues périodes.

Fonctionnement de Lambda

Lorsque vous utilisez Lambda, vous n'êtes responsable que de votre code. Lambda exécute le code sur une infrastructure informatique à haute disponibilité et gère toutes les ressources de calcul, y compris la maintenance des serveurs et du système d'exploitation, l'allocation et automatique de capacité, la mise à l'échelle automatique et la journalisation.

Lambda étant un service de calcul sans serveur piloté par les événements, il utilise une approche de programmation différente de celle des applications Web traditionnelles. Le modèle suivant illustre le fonctionnement de Lambda :

1. Vous écrivez et organisez votre code dans des fonctions Lambda, qui sont les éléments de base que vous utilisez pour créer une application Lambda.
2. Vous contrôlez la sécurité et l'accès via des autorisations Lambda, en utilisant des rôles d'exécution pour gérer les AWS services avec lesquels vos fonctions peuvent interagir et les politiques de ressources peuvent interagir avec votre code.
3. Les sources d'événements et AWS les services déclenchent vos fonctions Lambda, en transmettant les données d'événements au format JSON, que vos fonctions traitent (cela inclut les mappages de sources d'événements).
4. Lambda exécute votre code avec des environnements d'exécution spécifiques au langage (tels que Node.js Python) dans des environnements d'exécution qui empaquetent votre environnement d'exécution, vos couches et vos extensions.

> **Tip**
>
> Pour apprendre à créer des solutions sans serveur, consultez le Guide du développeur sans serveur.

Fonctionnalités principales

Configurez, contrôlez et déployez des applications sécurisées :

- Variables d'environnement modifiez le comportement des applications sans nouveaux déploiements de code.
- Versions testez les nouvelles fonctionnalités en toute sécurité tout en maintenant des environnements de production stables.

- Layers optimisez la réutilisation et la maintenance du code en partageant des composants communs entre plusieurs fonctions.
- Signature de code appliquez la conformité en matière de sécurité en veillant à ce que seul le code approuvé atteigne les systèmes de production.

Mise à l'échelle et fonctionnement fiable :

- Les contrôles de simultanéité et de mise à l'échelle gèrent avec précision la réactivité des applications et l'utilisation des ressources lors des pics de trafic.
- SnapStart réduisez considérablement les temps de démarrage à froid. Lambda SnapStart peut fournir des performances de démarrage inférieures à une seconde, généralement sans modification du code de votre fonction d'événement.
- Streaming des réponses optimisez les performances des fonctions en fournissant progressivement des données utiles volumineuses pour un traitement en temps réel.
- Images de conteneurs empaquetez des fonctions avec des dépendances complexes à l'aide des flux de travail de conteneurs.

Connectez et intégrez en toute simplicité :

- Les réseaux VPC sécurisent les ressources sensibles et les services internes.
- Systèmes de fichiers une intégration qui partage des données persistantes et gère les opérations dynamiques lors des invocations de fonctions.
- URL de fonctions créez des API et des points de terminaison destinés au public sans services supplémentaires.
- Extensions augmentez les fonctions grâce à des outils opérationnels, de surveillance et de sécurité.

Informations connexes

- Pour plus d'informations sur la manière dont Lambda fonctionne, consultez Fonctionnement de Lambda.
- Pour commencer à utiliser Lambda, consultez Création de votre première fonction Lambda.
- Pour obtenir une liste d'exemples d'applications, consultez Commencer avec des exemples d'applications et de modèles.

Fonctionnement de Lambda

Les fonctions Lambda sont les blocs de construction de base que vous utilisez pour créer des applications Lambda. Pour écrire des fonctions, il est essentiel de comprendre les concepts et composants fondamentaux du modèle de programmation Lambda. Cette section présente les éléments fondamentaux que vous devez connaître pour commencer à créer des applications sans serveur avec Lambda.

- Fonctions Lambda et gestionnaires de fonctions- Une fonction Lambda est un petit bloc de code qui s'exécute en réponse à des événements. Les fonctions sont les éléments de base que vous utilisez pour créer des applications. Les gestionnaires de fonctions constituent le point d'entrée pour les objets d'événements traités par le code de votre fonction Lambda.
- Environnement d'exécution et exécutions Lambda : les environnements d'exécution Lambda gèrent les ressources nécessaires à l'exécution de votre fonction. Les runtimes sont les environnements spécifiques au langage dans lesquels vos fonctions s'exécutent.
- Événements et déclencheurs- D'autres Services AWS peuvent invoquer vos fonctions en réponse à des événements spécifiques.
- Autorisations et rôles Lambda- Contrôlez qui peut accéder à vos fonctions et avec quelles autres Services AWS fonctions peuvent interagir.

> **Tip**
>
> Si vous souhaitez commencer par comprendre le développement sans serveur de manière plus générale, consultez la section Comprendre la différence entre le développement traditionnel et le développement sans serveur dans le Guide du développeur AWS sans serveur.

Fonctions Lambda et gestionnaires de fonctions

Dans Lambda, les fonctions sont les blocs de construction fondamentaux que vous utilisez pour créer des applications. Une fonction Lambda est un morceau de code qui s'exécute en réponse à des événements, tels qu'un utilisateur sélectionnant un bouton sur un site Web ou un fichier chargé vers un compartiment Amazon Simple Storage Service (Amazon S3). Grâce à des fonctions durables, votre code peut suspendre l'exécution entre les étapes, en maintenant l'état automatiquement, ce qui en fait un outil idéal pour les flux de travail de longue durée tels que le traitement des commandes

ou la modération du contenu. Vous pouvez considérer une fonction comme une sorte de programme autonome possédant les propriétés suivantes.

Un gestionnaire de fonction Lambda est la méthode dans le code de votre fonction qui traite les événements. Lorsqu'une fonction s'exécute en réponse à un événement, Lambda exécute le gestionnaire de fonction. Les données relatives à l'événement à l'origine de l'exécution de la fonction sont transmises directement au gestionnaire. Là où le code d'une fonction Lambda peut contenir plusieurs méthodes ou fonctions, les fonctions Lambda ne peuvent avoir qu'un seul gestionnaire.

Pour créer une fonction Lambda, vous groupez le code de votre fonction et ses dépendances dans un package de déploiement. Lambda prend en charge deux types de packages de déploiement : les archives de fichier .zip et les images conteneurs.

- Une fonction a une tâche ou un objectif spécifique
- Elle ne s'exécute que lorsque cela est nécessaire en réponse à des événements spécifiques
- Elle s'arrête automatiquement lorsqu'elle a terminé

Environnement d'exécution et exécutions Lambda

Les fonctions Lambda s'exécutent dans un environnement d'exécution sécurisé et isolé que Lambda gère pour vous. Pour des fonctions durables, l'environnement d'exécution inclut des composants supplémentaires pour la gestion de l'état et la coordination des flux de travail. L'environnement d'exécution gère les processus et les ressources nécessaires à l'exécution de votre fonction. Lorsqu'une fonction est invoquée pour la première fois, Lambda crée un nouvel environnement d'exécution dans lequel la fonction doit s'exécuter. Une fois l'exécution de la fonction terminée, Lambda n'arrête pas immédiatement l'environnement d'exécution ; si la fonction est à nouveau invoquée, Lambda peut réutiliser l'environnement d'exécution existant.

L'environnement d'exécution Lambda contient également un environnement d'exécution spécifique au langage (runtime), qui relaie les informations d'un événement et les réponses entre Lambda et votre fonction. Lambda fournit un certain nombre d'environnements d'exécution gérés pour les langages de programmation les plus courants, ou vous pouvez créer les vôtres.

Pour les environnements d'exécution gérés, Lambda applique automatiquement les mises à jour de sécurité et correctifs aux fonctions lors de l'exécution.

Événements et déclencheurs

Vous pouvez également invoquer une fonction Lambda directement avec la console Lambda, AWS CLI ou l'un des kits de développement logiciel (SDK)AWS. Dans une application de production, il est plus courant que votre fonction soit invoquée par une autre Service AWS en réponse à un événement particulier. Par exemple, vous souhaiterez peut-être qu'une fonction s'exécute chaque fois qu'un élément est ajouté à une table Amazon DynamoDB.

Pour que votre fonction réagisse aux événements, vous devez configurer un déclencheur. Un déclencheur connecte votre fonction à une source d'événements, et votre fonction peut avoir plusieurs déclencheurs. Lorsqu'un événement se produit, Lambda reçoit les données de l'événement sous forme de document JSON et les convertit en un objet que votre code peut traiter. Vous pouvez définir le format JSON suivant pour votre événement, et l'environnement d'exécution Lambda convertit ce JSON en objet avant de le transmettre au gestionnaire de votre fonction.

Exampleévénement lambda personnalisé

```
{
  "Location": "SEA",
  "WeatherData":{
    "TemperaturesF":{
      "MinTempF": 22,
      "MaxTempF": 78
    },
    "PressuresHPa":{
      "MinPressureHPa": 1015,
      "MaxPressureHPa": 1027
    }
  }
}
```

Les services de streaming et de file d'attente tels qu'Amazon Kinesis ou Amazon SQS utilisent un mappage de source d'événements au lieu d'un déclencheur standard. Les mappages des sources d'événements interrogent la source à la recherche de nouvelles données, regroupent les enregistrements, puis invoquent votre fonction avec les événements par lots. Pour de plus amples informations, veuillez consulter Différence entre les mappages de sources d'événements et les déclencheurs directs.

Pour comprendre le fonctionnement d'un déclencheur, commencez par suivre le didacticiel Utiliser un déclencheur Amazon S3 ou, pour obtenir une présentation générale de l'utilisation des déclencheurs

et des instructions sur la création d'un déclencheur à l'aide de la console Lambda, consultez Intégration d'autres services.

Autorisations et rôles Lambda

Pour Lambda, il existe deux principaux types d'autorisations que vous devez configurer :

- Autorisations dont votre fonction a besoin pour accéder à d'autres Services AWS
- Autorisations dont les autres utilisateurs Services AWS ont besoin pour accéder à votre fonction

Les sections suivantes décrivent ces deux types d'autorisations et décrivent les meilleures pratiques pour appliquer les autorisations de moindre privilège.

Autorisations permettant aux fonctions d'accéder à d'autres AWS resources

Les fonctions Lambda doivent souvent accéder à d'autres AWS ressources et effectuer des actions sur celles-ci. Par exemple, une fonction peut lire des éléments d'une table DynamoDB, stocker un objet dans un compartiment S3 ou écrire dans une file d'attente Amazon SQS. Pour donner aux fonctions les autorisations dont elles ont besoin pour effectuer ces actions, vous utilisez un rôle d'exécution.

Un rôle d'exécution Lambda est un type particulier de rôle Gestion des identités et des accès AWS (IAM), une identité que vous créez dans votre compte et à laquelle sont associées des autorisations spécifiques définies dans une politique.

Chaque fonction Lambda doit avoir un rôle d'exécution, et un même rôle peut être utilisé par plusieurs fonctions. Lorsqu'une fonction est invoquée, Lambda assume le rôle d'exécution de la fonction et est autorisé à effectuer les actions définies dans la politique du rôle.

Lorsque vous créez une fonction dans la console Lambda, Lambda crée automatiquement un rôle d'exécution pour votre fonction. La politique du rôle confère à votre fonction les autorisations de base nécessaires pour écrire les résultats des CloudWatch journaux dans Amazon Logs. Pour autoriser votre fonction à effectuer des actions sur d'autres AWS ressources, vous devez modifier le rôle afin d'ajouter les autorisations supplémentaires.

Le moyen le plus simple d'ajouter des autorisations consiste à utiliser une politique AWS gérée. Les politiques gérées sont créées et administrées par AWS et fournissent des autorisations pour de nombreux cas d'utilisation courants. Par exemple, si votre fonction effectue des opérations CRUD sur une table DynamoDB, vous pouvez ajouter la AmazonDynamoDBFullAccess politique à votre rôle.

Autorisations permettant à d'autres utilisateurs et ressources d'accéder à votre fonction

Pour accorder d'autres Service AWS autorisations d'accès à votre fonction Lambda, vous utilisez une politique basée sur les ressources. Dans IAM, les politiques basées sur les ressources sont attachées à une ressource (dans ce cas, votre fonction Lambda) et définissent qui peut accéder à la ressource et quelles actions peuvent être effectuées.

Pour Service AWS qu'un autre utilisateur puisse invoquer votre fonction via un déclencheur, la politique basée sur les ressources de votre fonction doit accorder à ce service l'autorisation d'utiliser l'action. `lambda:InvokeFunction` Si vous créez le déclencheur à l'aide de la console, Lambda ajoute automatiquement cette autorisation pour vous.

Pour autoriser d'autres AWS utilisateurs à accéder à votre fonction, vous pouvez le définir dans la politique basée sur les ressources de votre fonction exactement de la même manière que pour une autre Service AWS ou ressource. Vous pouvez également utiliser une politique basée sur l'identité associée à l'utilisateur.

Bonnes pratiques relatives aux autorisations Lambda

Lorsque vous définissez des autorisations avec des stratégies IAM, la bonne pratique de sécurité est d'accorder uniquement les autorisations nécessaires à l'exécution d'une seule tâche. C'est ce que l'on appelle le principe du moindre privilège. Pour commencer à accorder des autorisations pour votre fonction, vous pouvez choisir d'utiliser une politique AWS gérée. Les politiques gérées peuvent être le moyen le plus rapide et le plus simple d'accorder des autorisations pour effectuer une tâche, mais elles peuvent également inclure d'autres autorisations dont vous n'avez pas besoin. À mesure que vous passez du stade initial du développement aux tests et à la production, nous vous recommandons de limiter les autorisations aux seules autorisations nécessaires en définissant vos propres politiques gérées par le client.

Le même principe s'applique lorsque vous accordez des autorisations d'accès à votre fonction à l'aide d'une politique basée sur les ressources. Par exemple, si vous souhaitez autoriser Amazon S3 à invoquer votre fonction, il est recommandé de limiter l'accès à des compartiments individuels, ou à des compartiments en particulier Comptes AWS, plutôt que d'accorder des autorisations générales au service S3.

Exécution de code avec Lambda

Lorsque vous écrivez une fonction Lambda, vous créez du code qui s'exécute dans un environnement sans serveur unique. Comprendre comment Lambda exécute réellement votre code implique deux aspects essentiels : le modèle de programmation qui définit la façon dont votre code interagit avec Lambda, et le cycle de vie de l'environnement d'exécution qui détermine la manière dont Lambda gère l'environnement d'exécution de votre code.

Le modèle de programmation Lambda

Le modèle de programmation fonctionne comme un ensemble de règles communes régissant le fonctionnement de Lambda avec votre code, que vous écriviez en Python, en Java ou dans tout autre langage pris en charge. Le modèle de programmation inclut votre environnement d’exécution et votre gestionnaire.

Pour les fonctions sans exécution durable :

1. Lambda reçoit un événement.
2. Lambda utilise le runtime pour préparer l'événement dans un format que votre code peut utiliser.
3. L’environnement d’exécution envoie l’événement formaté à votre gestionnaire.
4. Votre gestionnaire traite l'événement en utilisant le code que vous avez écrit.

Le gestionnaire, auquel Lambda envoie des événements à traiter par votre code, est essentiel à ce modèle. Considérez-le comme le point d’entrée de votre code. Lorsque Lambda reçoit un événement, il le transmet à votre gestionnaire avec certaines informations contextuelles. Le gestionnaire exécute ensuite votre code pour traiter ces événements. Par exemple, il peut lire un fichier lorsqu’il est chargé sur Amazon S3, analyser une image ou mettre à jour une base de données. Une fois que votre code a fini de traiter un événement, le gestionnaire est prêt à traiter le suivant.

Le modèle d’exécution Lambda

Alors que le modèle de programmation définit la manière dont Lambda interagit avec votre code, l'environnement d'exécution est l'endroit où Lambda exécute réellement votre fonction. Il s'agit d'un espace de calcul sécurisé et isolé créé spécifiquement pour votre fonction.

Chaque environnement suit un cycle de vie :

1. Initialisation : configuration de l'environnement et chargement du code

2. Invocation : exécution unique du code de fonction
3. Arrêt : nettoyage de l'environnement

Cet environnement gère les aspects importants de l’exécution de votre fonction. Il fournit à votre fonction de la mémoire et un répertoire `/tmp` pour le stockage temporaire.

Présentation du modèle de programmation Lambda

Les fonctions d'événement Lambda s'exécutent par défaut pendant 15 minutes maximum par appel. Les invocations asynchrones et de mappage des sources d'événements (ESM) sur les instances gérées Lambda peuvent s'exécuter pendant 90 minutes maximum. Les fonctions durables peuvent fonctionner jusqu'à un an. Bien que les deux partagent des concepts fondamentaux, les fonctions durables ajoutent des fonctionnalités pour des flux de travail dynamiques et de longue durée.

Lambda fournit un modèle de programmation commun à tous les runtimes. Le modèle de programmation définit l'interface entre votre code et le système Lambda. Vous indiquez à Lambda le point d'entrée de votre fonction en définissant un gestionnaire dans la configuration de la fonction. Le runtime transmet les objets au gestionnaire qui contiennent l'événement d'invocation et le contexte, tels que le nom de la fonction et l'ID de la demande.

Pour Durable Functions, le gestionnaire reçoit également un DurableContext objet qui fournit :

- Capacités de point de contrôle via step ()
- Gestion de l'état d'attente via wait () et wait ForCallback ()
- Persistance automatique de l'état entre les invocations

Lorsque le gestionnaire termine le traitement du premier événement, le runtime lui en envoie un autre. Pour les fonctions durables, le gestionnaire peut suspendre l'exécution entre les étapes, et Lambda enregistre et restaure automatiquement l'état lorsque la fonction reprend. La classe de la fonction reste en mémoire, de sorte que les clients et variables déclarés en dehors de la méthode du gestionnaire dans le code d'initialisation peuvent être réutilisés. Pour économiser du temps de traitement sur les événements suivants, créez des ressources réutilisables telles que des clients AWS SDK lors de l'initialisation. Une fois initialisée, chaque instance de votre fonction peut traiter des milliers de demandes.

Votre fonction a également accès au stockage local dans le répertoire `/tmp`, un cache temporaire qui peut servir à plusieurs appels. Pour plus d’informations, consultez Environnement d’exécution.

Lorsque le suivi AWS X-Ray est activé, le runtime enregistre des sous-segments distincts pour l'initialisation et l'exécution.

Le moteur d'exécution capture les résultats de journalisation de votre fonction et les envoie à Amazon CloudWatch Logs. En plus de consigner la sortie de votre fonction, le runtime consigne également les entrées lorsque la fonction d'invocation démarre et se termine. Cela inclut un journal de rapport avec l'ID de demande, la durée facturée, la durée d'initialisation et d'autres détails. Si votre fonction génère une erreur, le runtime renvoie cette erreur au mécanisme d'appel.

> **Note**
>
> La journalisation est soumise à des quotas de CloudWatch journalisation. Les données des journaux peuvent être perdues en raison de la limitation ou, dans certains cas, lorsqu'une instance de votre fonction est arrêtée.

Principales différences en matière de fonctions durables :

- L'état est automatiquement conservé entre les étapes
- Les fonctions peuvent suspendre l'exécution sans consommer de ressources
- Les étapes sont automatiquement réessayées en cas d'échec
- Les progrès sont suivis par le biais de points de contrôle

Lambda met à l'échelle votre fonction en exécutant des instances supplémentaires à mesure que la demande augmente et en arrêtant des instances à mesure que la demande diminue. Ce modèle entraîne des variations dans l'architecture des applications, telles que :

- Sauf indication contraire, les demandes entrantes peuvent être traitées dans le désordre ou simultanément.
- Ne comptez pas sur la longévité des instances de votre fonction, stockez plutôt l'état de votre application ailleurs.
- Utilisez le stockage local et les objets de niveau classe afin d'améliorer les performances, mais réduisez au minimum la taille de votre package de déploiement et la quantité de données que vous transférez vers l'environnement d'exécution.

Pour une introduction pratique au modèle de programmation dans le langage de programmation de votre choix, consultez les sections suivantes.

- Création de fonctions événementielles Lambda avec Node.js
- Création de fonctions d'événement Lambda avec Python
- Création de fonctions d'événement Lambda avec Ruby
- Création de fonctions d'événement Lambda avec Java
- Création de fonctions événementielles Lambda avec Go
- Création de fonctions d'événement Lambda avec C#
- Création de fonctions d'événement Lambda avec PowerShell

Comprendre le cycle de vie de l'environnement d'exécution Lambda

Les environnements d'exécution Lambda exécutent des invocations de fonctions pendant 15 minutes maximum par défaut, et les fonctions durables peuvent s'exécuter jusqu'à un an. Les fonctions durables partagent le même cycle de vie de base et ajoutent des fonctionnalités de gestion des états pour les flux de travail de longue durée.

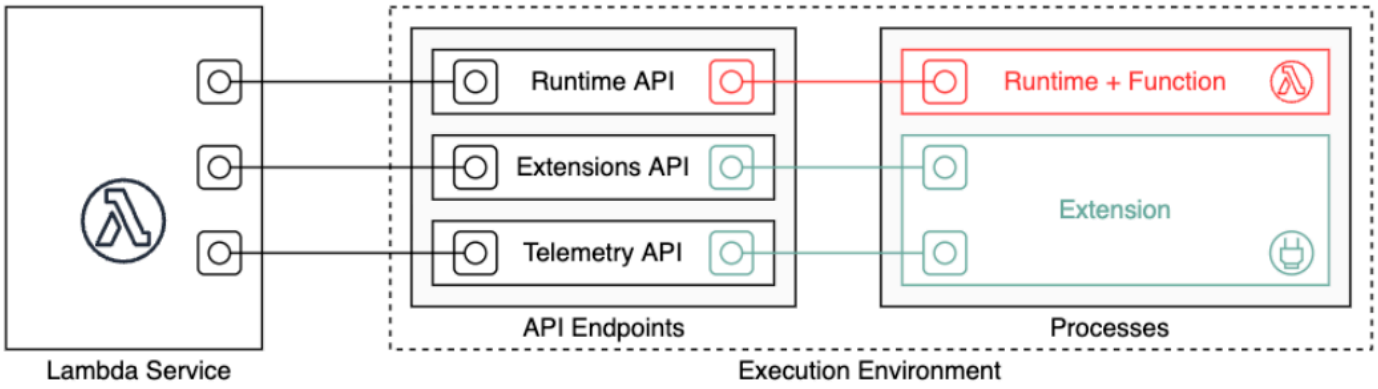
Lambda invoque votre fonction dans un environnement d'exécution, qui fournit un environnement d'exécution sécurisé et isolé. L'environnement d'exécution gère les ressources nécessaires à l'exécution de votre fonction. L'environnement d'exécution prend également en charge le cycle de vie pour l'exécution de la fonction et pour toutes les extensions externes associées à votre fonction.

Pour Durable Functions, l'environnement d'exécution inclut des composants supplémentaires pour :

- Persistance de l'état entre les étapes
- Gestion des points de contrôle
- Coordination de l'état d'attente
- Suivi des progrès

> **Environnement d'exécution des instances gérées Lambda**
>
> Si vous utilisez des instances gérées Lambda, l'environnement d'exécution présente des différences importantes par rapport aux fonctions Lambda (par défaut). Les instances gérées prennent en charge les appels simultanés, utilisent un modèle de cycle de vie différent et s'exécutent sur une infrastructure appartenant au client. Pour des informations détaillées sur l'environnement d'exécution des instances gérées, consultezComprendre l'environnement d'exécution des instances gérées Lambda.

L'exécution de la fonction communique avec Lambda à l'aide de l'API d'exécution. Les extensions communiquent avec Lambda à l'aide de l'API d'extensions. Les extensions peuvent également recevoir des messages de journal et d'autres télémétries de la fonction en utilisant l'API de télémétrie.



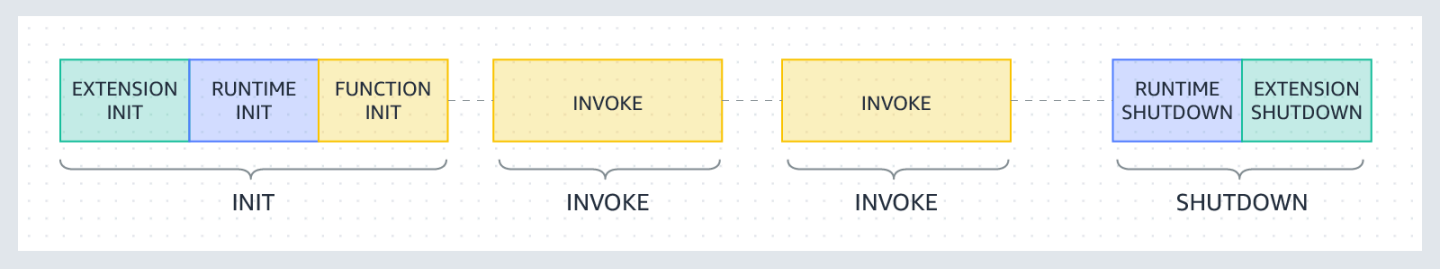
Lorsque vous créez votre fonction Lambda, vous précisez des informations de configuration, telles que la quantité de mémoire disponible et le temps d'exécution maximum autorisé pour votre fonction. Lambda utilise ces informations pour configurer l'environnement d'exécution.

L'exécution de la fonction et chaque extension externe sont des processus qui s'exécutent dans l'environnement d'exécution. Les autorisations, les ressources, les informations d'identification et les variables d'environnement sont partagées entre la fonction et les extensions.

Rubriques

- Cycle de vie d'un environnement d'exécution Lambda
- Démarrages à froid et latence
- Réduction des démarrages à froid avec la simultanéité provisionnée
- Optimisation de l'initialisation statique

Cycle de vie d'un environnement d'exécution Lambda



Chaque phase commence par un événement que Lambda envoie à l'exécution et à toutes les extensions enregistrées. L'exécution et chaque extension indiquent la fin de l'opération en envoyant une demande d'API `Next`. Lambda gèle l'environnement d'exécution lorsque l'exécution de chaque extension est terminée, et qu'il n'y a pas d'événement en attente.

Les phases du cycle de vie de Durable Functions incluent :

- Init : initialisation standard et configuration d'état durable
- Invoke : peut inclure des exécutions en plusieurs étapes avec pointage automatique
- Attendre : la fonction peut suspendre l'exécution sans consommer de ressources
- Reprise : la fonction redémarre depuis le dernier point de contrôle
- Arrêt : nettoyage de l'état durable et des ressources

Rubriques

- Phase d'initialisation
- Échecs pendant la phase d'initialisation
- Phase de restauration (Lambda uniquement SnapStart)
- Phase d'invocation
- Échecs pendant la phase d'invocation
- Phase d'arrêt

Phase d'initialisation

Dans la phase `Init`, Lambda effectue trois tâches :

- Démarrage de toutes les extensions (`Extension init`)
- Amorçage de l'exécution (`Runtime init`)
- Exécution du code statique de la fonction (`Function init`)
- Exécutez tous les hooks d'exécution avant le point de contrôle (Lambda uniquement) SnapStart

La phase `Init` se termine lorsque l'exécution et toutes les extensions signalent qu'elles sont prêtes en envoyant une demande d'API `Next`. La phase `Init` est limitée à 10 secondes. Si les trois tâches ne se terminent pas dans les 10 secondes, Lambda relance la phase `Init` au moment de la première invocation de fonction avec le délai d'attente de fonction configuré.

Lorsque SnapStart est activé, la phase `Init` se produit lorsque vous publiez une version de la fonction. Lambda enregistre un instantané de l'état de la mémoire et du disque de l'environnement d'exécution initialisé, fait persister l'instantané chiffré et le met en cache pour un accès à faible latence. Si vous avez un hook d'environnement d'exécution avant le point de contrôle, le code s'exécute alors à la fin de la phase `Init`.

> **Note**
>
> Le délai d'expiration de 10 secondes ne s'applique pas aux fonctions qui utilisent la simultanéité provisionnée SnapStart ou les instances gérées Lambda. Pour les fonctions de simultanéité provisionnée et d'instances gérées, votre code d'initialisation peut s'exécuter pendant 15 minutes maximum. SnapStart Le délai d'attente est de 130 secondes ou le délai d'expiration de la fonction configurée (900 secondes au maximum), la valeur la plus élevée étant retenue.

Lorsque vous utilisez la simultanéité provisionnée, Lambda initialise l'environnement d'exécution lorsque vous configurez les paramètres du PC pour une fonction. Lambda garantit également que les environnements d'exécution initialisés sont toujours disponibles avant les invocations. Il se peut que vous constatiez des écarts entre les phases d'invocation et d'initialisation de votre fonction. En fonction de l'exécution et de la configuration de la mémoire de votre fonction, vous pouvez également constater une latence variable lors du premier appel dans un environnement d'exécution initialisé.

Pour les fonctions utilisant la simultanéité à la demande, Lambda peut parfois initialiser les environnements d'exécution avant les demandes d'invocation. Lorsque cela se produit, vous pouvez également observer un intervalle de temps entre les phases d'initialisation et d'invocation de votre fonction. Nous vous recommandons de ne pas dépendre de ce comportement.

Échecs pendant la phase d'initialisation

Si une fonction se bloque ou expire pendant la phase `Init`, Lambda émet des informations d'erreur dans le journal `INIT_REPORT`.

Example— Journal INIT_REPORT pour le délai d'expiration

```
INIT_REPORT Init Duration: 1236.04 ms Phase: init Status: timeout
```

Example— Journal INIT_REPORT en cas d'échec de l'extension

```
INIT_REPORT Init Duration: 1236.04 ms Phase: init Status: error Error Type:
 Extension.Crash
```

Si la `Init` phase est réussie, Lambda n'émet le `INIT_REPORT` journal que si la simultanéité SnapStartprovisionnée est activée. SnapStart et les fonctions de simultanéité provisionnées émettent toujours. `INIT_REPORT` Pour plus d'informations, consultez Surveillance pour Lambda SnapStart.

Phase de restauration (Lambda uniquement SnapStart)

Lorsque vous appelez une SnapStartfonction pour la première fois et que celle-ci évolue, Lambda reprend les nouveaux environnements d'exécution à partir de l'instantané persistant au lieu d'initialiser la fonction à partir de zéro. Si vous avez un hook d'exécution après restauration, le code s'exécute à la fin de la phase `Restore`. Vous êtes facturé pour la durée des hooks d'exécution après restauration. L'exécution doit se charger et les hooks d'exécution après restauration doivent se terminer dans le délai imparti (10 secondes). Sinon, vous obtiendrez un SnapStartTimeoutException. Lorsque la phase `Restore` se termine, Lambda invoque le gestionnaire de fonction (Phase d'invocation).

Échecs pendant la phase de restauration

Si la phase `Restore` échoue, Lambda émet des informations d'erreur dans le journal `RESTORE_REPORT`.

Example— Journal RESTORE_REPORT pour le délai d'expiration

```
RESTORE_REPORT Restore Duration: 1236.04 ms Status: timeout
```

Example— Journal RESTORE_REPORT en cas d'échec du hook d'exécution

```
RESTORE_REPORT Restore Duration: 1236.04 ms Status: error Error Type: Runtime.ExitError
```

Pour plus d'informations sur le journal `RESTORE_REPORT`, consultez Surveillance pour Lambda SnapStart.

Phase d'invocation

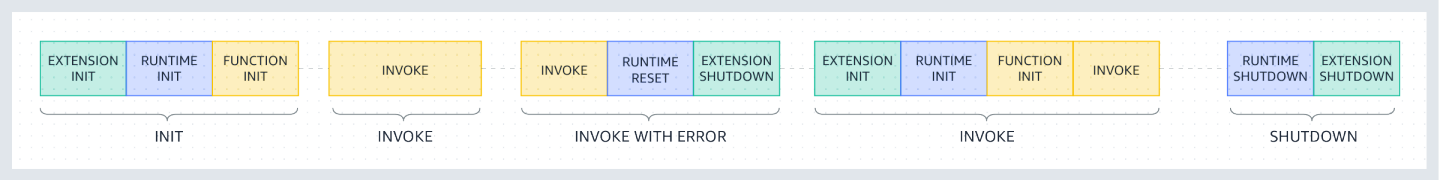
Quand une fonction Lambda est invoquée en réponse à une demande d'API `Next`, Lambda envoie un événement `Invoke` à l'exécution et à chaque extension.

Le paramètre d'expiration de la fonction limite la durée de l'ensemble de la phase `Invoke`. Par exemple, si vous définissez le délai d'expiration de la fonction sur 360 secondes, la fonction et toutes les extensions doivent être terminées dans un délai de 360 secondes. Notez qu'il n'y a pas de phase post-invocation indépendante. La durée correspond à la somme de tous les temps d'invocation (exécution + extensions) et n'est calculée que lorsque l'exécution de la fonction et de toutes les extensions est terminée.

La phase d'invocation prend fin lorsque l'exécution et toutes les extensions signalent qu'ils ont terminé en envoyant une demande d'API `Next`.

Échecs pendant la phase d'invocation

Si la fonction Lambda se bloque ou expire pendant la phase `Invoke`, Lambda réinitialise l'environnement d'exécution. Le diagramme suivant illustre le comportement de l'environnement d'exécution Lambda en cas d'échec de l'invocation :



Dans le diagramme précédent :

- La première phase est la phase INIT, qui s'exécute sans erreur.
- La deuxième phase est la phase INVOKE, qui s'exécute sans erreur.
- Supposons qu'à un moment donné, votre fonction rencontre un échec d'invocation (les causes courantes incluent les expirations de délai des fonctions, les erreurs d'exécution, l'épuisement de la mémoire, les problèmes de connectivité VPC, les erreurs d'autorisation, les limites de simultanéité et divers problèmes de configuration). Pour connaître la liste complète des échecs d'invocation possibles, consultez the section called "Invocation". La troisième phase, intitulée INVOKE WITH ERROR, illustre ce scénario.

  Lorsque cela se produit, le service Lambda effectue une réinitialisation. La réinitialisation se comporte comme un événement `Shutdown`. Lambda commence par arrêter l'exécution, puis envoie un événement `Shutdown` à chaque extension externe enregistrée. L'événement comprend le motif de l'arrêt. Si cet environnement est utilisé pour une nouvelle invocation, Lambda réinitialise l'extension et l'exécution en même temps que l'invocation suivante.

  Notez que la réinitialisation Lambda n'efface pas le contenu du `/tmp` répertoire avant la phase d'initialisation suivante. Ce comportement est cohérent avec la phase d'arrêt normale.

> **Note**
>
> AWS met actuellement en œuvre des modifications du service Lambda. En raison de ces modifications, vous pouvez constater des différences mineures entre la structure et le contenu des messages du journal système et des segments de trace émis par les différentes fonctions d'événement Lambda de votre ordinateur. Compte AWS
> Si la configuration du journal système de votre fonction est définie sur du texte brut, cette modification affecte les messages de journal capturés dans CloudWatch les journaux lorsque votre fonction rencontre un échec d'appel. Les exemples suivants montrent les sorties des journaux dans les anciens et les nouveaux formats.
> Ces modifications seront mises en œuvre au cours des prochaines semaines, et toutes les fonctions, Régions AWS sauf en Chine et dans les GovCloud régions, passeront à l'utilisation du nouveau format des messages de journal et des segments de trace.

Example CloudWatch Journalise la sortie du journal (exécution ou crash de l'extension) - ancien style

```
START RequestId: c3252230-c73d-49f6-8844-968c01d1e2e1 Version: $LATEST
RequestId: c3252230-c73d-49f6-8844-968c01d1e2e1 Error: Runtime exited without
 providing a reason
Runtime.ExitError
END RequestId: c3252230-c73d-49f6-8844-968c01d1e2e1
REPORT RequestId: c3252230-c73d-49f6-8844-968c01d1e2e1 Duration: 933.59 ms Billed
 Duration: 934 ms Memory Size: 128 MB Max Memory Used: 9 MB
```

Example CloudWatch Enregistre la sortie du journal (délai d'expiration de la fonction) - ancien style

```
START RequestId: b70435cc-261c-4438-b9b6-efe4c8f04b21 Version: $LATEST
2024-03-04T17:22:38.033Z b70435cc-261c-4438-b9b6-efe4c8f04b21 Task timed out after
 3.00 seconds
END RequestId: b70435cc-261c-4438-b9b6-efe4c8f04b21
REPORT RequestId: b70435cc-261c-4438-b9b6-efe4c8f04b21 Duration: 3004.92 ms Billed
 Duration: 3117 ms Memory Size: 128 MB Max Memory Used: 33 MB Init Duration: 111.23
 ms
```

Le nouveau format des CloudWatch journaux inclut un `status` champ supplémentaire dans la REPORT ligne. Dans le cas d'un incident d'exécution ou d'extension, la ligne REPORT inclut également un champ `ErrorType`.

Example CloudWatch Journalise la sortie du journal (exécution ou crash de l'extension) - nouveau style

```
START RequestId: 5b866fb1-7154-4af6-8078-6ef6ca4c2ddd Version: $LATEST
END RequestId: 5b866fb1-7154-4af6-8078-6ef6ca4c2ddd
REPORT RequestId: 5b866fb1-7154-4af6-8078-6ef6ca4c2ddd Duration: 133.61 ms Billed
 Duration: 214 ms Memory Size: 128 MB Max Memory Used: 31 MB Init Duration: 80.00
 ms Status: error Error Type: Runtime.ExitError
```

Example CloudWatch Enregistre la sortie du journal (délai d'expiration de la fonction) - nouveau style

```
START RequestId: 527cb862-4f5e-49a9-9ae4-a7edc90f0fda Version: $LATEST
END RequestId: 527cb862-4f5e-49a9-9ae4-a7edc90f0fda
REPORT RequestId: 527cb862-4f5e-49a9-9ae4-a7edc90f0fda Duration: 3016.78 ms Billed
 Duration: 3101 ms Memory Size: 128 MB Max Memory Used: 31 MB Init Duration: 84.00
 ms Status: timeout
```

- La quatrième phase représente la phase INVOKE qui suit immédiatement un échec de l'invocation. Ici, Lambda initialise à nouveau l'environnement en relançant la phase INIT. Cela s'appelle une init supprimée.

  Lorsque des initialisations supprimées se produisent, Lambda ne signale pas explicitement une phase d'initialisation supplémentaire dans Logs. CloudWatch Au lieu de cela, vous remarquerez peut-être que la durée indiquée dans la ligne REPORT inclut une durée INIT supplémentaire plus la durée INVOKE. Supposons, par exemple, que les connexions suivantes s'affichent CloudWatch :

  ```
  2022-12-20T01:00:00.000-08:00 START RequestId: XXX Version: $LATEST
  2022-12-20T01:00:02.500-08:00 END RequestId: XXX
  2022-12-20T01:00:02.500-08:00 REPORT RequestId: XXX Duration: 3022.91 ms
  Billed Duration: 3000 ms Memory Size: 512 MB Max Memory Used: 157 MB
  ```

  Dans cet exemple, la différence entre les horodatages REPORT et START est de 2,5 secondes. Cela ne correspond pas à la durée rapportée de 3022,91 millisecondes, car cela ne prend pas

en compte l'INIT supplémentaire (init supprimé) que Lambda a effectué. Dans cet exemple, vous pouvez en déduire que la phase INVOKE réelle a duré 2,5 secondes.

Pour plus d'informations sur ce comportement, vous pouvez utiliser la Accès aux données de télémétrie en temps réel pour les extensions à l'aide de l'API de télémétrie. L'API de télémétrie émet des événements `INIT_START`, `INIT_RUNTIME_DONE` et `INIT_REPORT` avec `phase=invoke` chaque fois que des inits supprimés se produisent entre les phases d'invocation.

- La cinquième phase représente la phase SHUTDOWN, qui s'exécute sans erreur.

Phase d'arrêt

Quand Lambda est sur le point d'arrêter l'exécution, il envoie un événement `Shutdown` à chaque extension externe enregistrée. Les extensions peuvent utiliser ce temps pour les tâches de nettoyage final. L'événement `Shutdown` est une réponse à une `Next`demande d'API.

Limite de durée : la durée maximale de la phase `Shutdown` dépend de la configuration des extensions enregistrées :

- 0 ms : fonction sans extension enregistrée
- 500 ms : fonction avec une extension interne enregistrée.
- 2 000 ms : fonction avec une ou plusieurs extensions externes enregistrées.

Si l'environnement d'exécution ou une extension ne répondent pas à l'événement `Shutdown` dans cette limite de temps, Lambda met fin au processus à l'aide d'un signal `SIGKILL`.

Lorsque la fonction et toutes les extensions ont pris fin, Lambda conserve l'environnement d'exécution pendant un certain temps en prévision d'une autre invocation de fonction. Cependant, Lambda met fin aux environnements d'exécution toutes les quelques heures pour permettre les mises à jour et la maintenance de l'environnement d'exécution, même pour les fonctions invoquées en continu. Vous ne devez pas partir du principe que l'environnement d'exécution sera conservé indéfiniment. Pour plus d'informations, consultez Implémenter l'absence d'état dans les fonctions.

Lorsque la fonction est à nouveau invoquée, Lambda décongèle l'environnement pour le réutiliser. La réutilisation de l'environnement d'exécution a les conséquences suivantes :

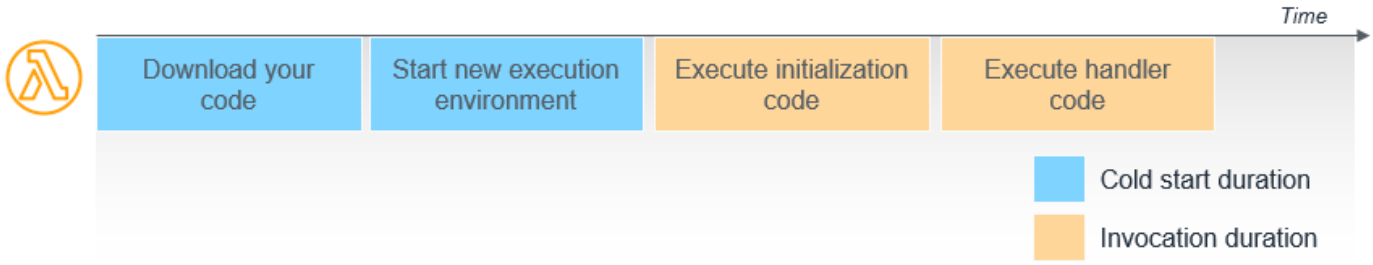
- Les objets déclarés en dehors de la méthode de gestionnaire de la fonction restent initialisés, ce qui fournit une optimisation supplémentaire lorsque la fonction est invoquée à nouveau. Par exemple, si votre fonction Lambda établit une connexion de base de données, au lieu de rétablir

la connexion, la connexion d'origine est utilisée dans les invocations suivantes. Nous vous recommandons d'ajouter une logique dans votre code pour vérifier s'il existe une connexion avant d'en créer une nouvelle.

- Chaque environnement d'exécution fournit entre 512 Mo et 10 240 Mo, par incréments de 1 Mo d'espace disque dans le répertoire `/tmp`. Le contenu du répertoire est conservé lorsque l'environnement d'exécution est gelé, fournissant ainsi un cache temporaire qui peut servir à plusieurs invocations. Vous pouvez ajouter du code pour vérifier si le cache contient les données que vous avez stockées. Pour de plus amples informations sur les limites de taille de déploiement, veuillez consulter Quotas Lambda.
- Les processus en arrière-plan ou les rappels qui ont été initiés par votre fonction Lambda et qui ne sont pas terminés à la fin de l'exécution de la fonction reprennent si Lambda réutilise l'environnement d'exécution. Assurez-vous que les processus d'arrière-plan ou les rappels dans votre code se terminent avant que l'exécution du code ne prenne fin.

Démarrages à froid et latence

Lorsque Lambda reçoit une demande pour exécuter une fonction via l'API Lambda, le service prépare d'abord un environnement d'exécution. Au cours de cette phase d'initialisation, le service télécharge votre code, démarre l'environnement et exécute tout code d'initialisation en dehors du gestionnaire principal. Enfin, Lambda exécute le code du gestionnaire.



Dans ce schéma, les deux premières étapes du téléchargement du code et de la configuration de l'environnement sont souvent appelées « démarrage à froid ». Cette durée vous est facturée, et ajoute de la latence à la durée globale de votre invocation.

Une fois l'invocation terminée, l'environnement d'exécution est gelé. Pour améliorer la gestion des ressources et les performances, Lambda retient l'environnement d'exécution pendant une période. Pendant ce temps, si une autre demande arrive pour la même fonction, Lambda peut réutiliser l'environnement. Cette deuxième demande se termine généralement plus rapidement, étant

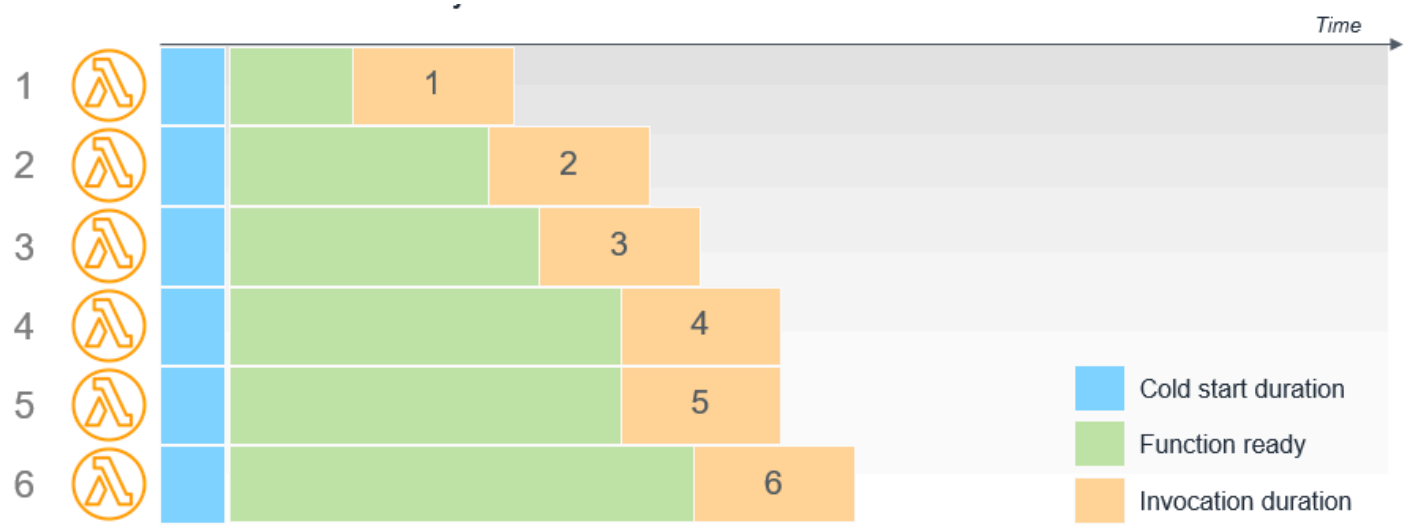
donné que l'environnement d'exécution est déjà entièrement configuré. C'est ce qu'on appelle un « démarrage à chaud ».

Les démarrages à froid concernent moins de 1 % des invocations. La durée d'un démarrage à froid varie de moins de 100 ms à plus d'une seconde. Les démarrages à froid concernent plus souvent les fonctions de développement et de test que les charges de travail de production. Cela est dû au fait que les fonctions de développement et de test sont généralement invoquées moins fréquemment.

Réduction des démarrages à froid avec la simultanéité provisionnée

Si vous avez besoin d'heures de démarrage des fonctions prévisibles pour votre charge de travail, la simultanéité provisionnée est la solution recommandée pour garantir la latence la plus faible possible. Cette fonctionnalité pré-initialise les environnements d'exécution, réduisant ainsi les démarrages à froid.

Par exemple, une fonction avec une simultanéité provisionnée de 6 dispose de 6 environnements d'exécution préparés.



Optimisation de l'initialisation statique

L'initialisation statique se produit avant que le code du gestionnaire ne commence à s'exécuter dans une fonction. Il s'agit du code d'initialisation que vous fournissez ; il se trouve en dehors du gestionnaire principal. Ce code est souvent utilisé pour importer des bibliothèques et des dépendances, définir les configurations et initialiser les connexions à d'autres services.

L'exemple Python suivant montre l'importation et la configuration de modules, ainsi que la création du client Amazon S3 pendant la phase d'initialisation, avant que la fonction `lambda_handler` ne s'exécute pendant l'invocation.

```
import os
import json
import cv2
import logging
import boto3

s3 = boto3.client('s3')
logger = logging.getLogger()
logger.setLevel(logging.INFO)

def lambda_handler(event, context):

  # Handler logic...
```

Le principal facteur de latence avant l'exécution d'une fonction provient du code d'initialisation. Ce code s'exécute lorsqu'un nouvel environnement d'exécution est créé pour la première fois. Le code d'initialisation n'est pas exécuté à nouveau si une invocation utilise un environnement d'exécution chaud. Les facteurs qui influent sur la latence du code d'initialisation sont notamment les suivants :

- la taille du package de fonctions, en termes de bibliothèques et de dépendances importées, et de couches Lambda ;
- la quantité de code et la tâche d'initialisation ;
- la performance des bibliothèques et des autres services lors de la configuration de connexions et d'autres ressources.

Les développeurs peuvent prendre un certain nombre de mesures pour optimiser la latence d'initialisation statique. Si une fonction comporte de nombreux objets et connexions, vous pouvez peut-être redéfinir l'architecture d'une seule fonction en plusieurs fonctions spécialisées. chacune plus petite et contenant chacun moins de code d'initialisation.

Il est important que les fonctions n'importent que les bibliothèques et les dépendances dont elles ont besoin. Par exemple, si vous utilisez Amazon DynamoDB uniquement dans AWS le SDK, vous pouvez avoir besoin d'un service individuel au lieu de l'intégralité du SDK. Voici trois exemples de comparaison :

```
// Instead of const AWS = require('aws-sdk'), use:
const DynamoDB = require('aws-sdk/clients/dynamodb')

// Instead of const AWSXRay = require('aws-xray-sdk'), use:
```

```
const AWSXRay = require('aws-xray-sdk-core')

// Instead of const AWS = AWSXRay.captureAWS(require('aws-sdk')), use:
const dynamodb = new DynamoDB.DocumentClient()
AWSXRay.captureAWSClient(dynamodb.service)
```

L’initialisation statique est aussi souvent le meilleur moment pour ouvrir des connexions à une base de données afin de permettre à une fonction de réutiliser les connexions via plusieurs invocations dans le même environnement d’exécution. Cependant, il se peut qu'un grand nombre d'objets ne soient utilisés que dans certains chemins d'exécution de votre fonction. Dans ce cas, vous pouvez charger de manière différée des variables dans la portée globale afin de réduire la durée d’initialisation statique.

Évitez les variables globales pour les informations spécifiques au contexte. Si votre fonction possède une variable globale qui n’est utilisée que pendant la durée de vie d’une seule invocation et qui est réinitialisée pour la prochaine invocation, utilisez une portée de variable locale au gestionnaire. Cela permet non seulement d’éviter les fuites de variables globales lors des invocations, mais également d’améliorer les performances d’initialisation statique.

Création d’architectures guidées par les événements avec Lambda

Un événement est tout ce qui déclenche l’exécution d’une fonction Lambda. Les événements peuvent déclencher une fonction Lambda de deux manières : par invocation directe (push) et par mappage des sources d'événements (pull).

De nombreux AWS services peuvent appeler directement vos fonctions Lambda. Ces services transmettent (push) des événements à votre fonction Lambda. Les événements qui déclenchent des fonctions peuvent être presque n'importe quoi, qu'il s'agisse d'une requête HTTP via API Gateway, d'un calendrier géré par EventBridge Scheduler, d'un AWS IoT événement ou d'un événement Amazon S3. Grâce au mappage des sources d’événements, Lambda récupère (pull) activement les événements d’une file d’attente ou d’un flux. Vous configurez Lambda pour vérifier les événements provenant d’un service pris en charge, et Lambda gère l’interrogation et l’invocation de votre fonction.

Lorsqu’ils sont transmis à votre fonction, les événements sont structurés au format JSON. La structure JSON varie en fonction du service qui la génère et du type d’événement. Alors que les appels de fonction Lambda peuvent durer jusqu'à 15 minutes par défaut, Lambda est particulièrement adapté aux appels courts d'une seconde ou moins. Cela est particulièrement vrai pour les architectures axées sur les événements, où chaque fonction Lambda est traitée comme un microservice chargé d’exécuter un ensemble restreint d’instructions spécifiques.

> **Note**
>
> Event-driven les architectures communiquent entre différents systèmes à l'aide de réseaux, ce qui introduit une latence variable. Pour les charges de travail nécessitant une très faible latence, telles que les systèmes de trading en temps réel, cette conception n'est peut-être pas le meilleur choix. Toutefois, pour les charges de travail hautement évolutives et disponibles, ou celles dont les modèles de trafic sont imprévisibles, les architectures guidées par les événements peuvent constituer un moyen efficace de répondre à ces demandes.

Rubriques

- Avantages des architectures guidées par les événements
- Trade-offs d'architectures pilotées par les événements
- Anti-patterns dans les applications Lambda-based pilotées par les événements

Avantages des architectures guidées par les événements

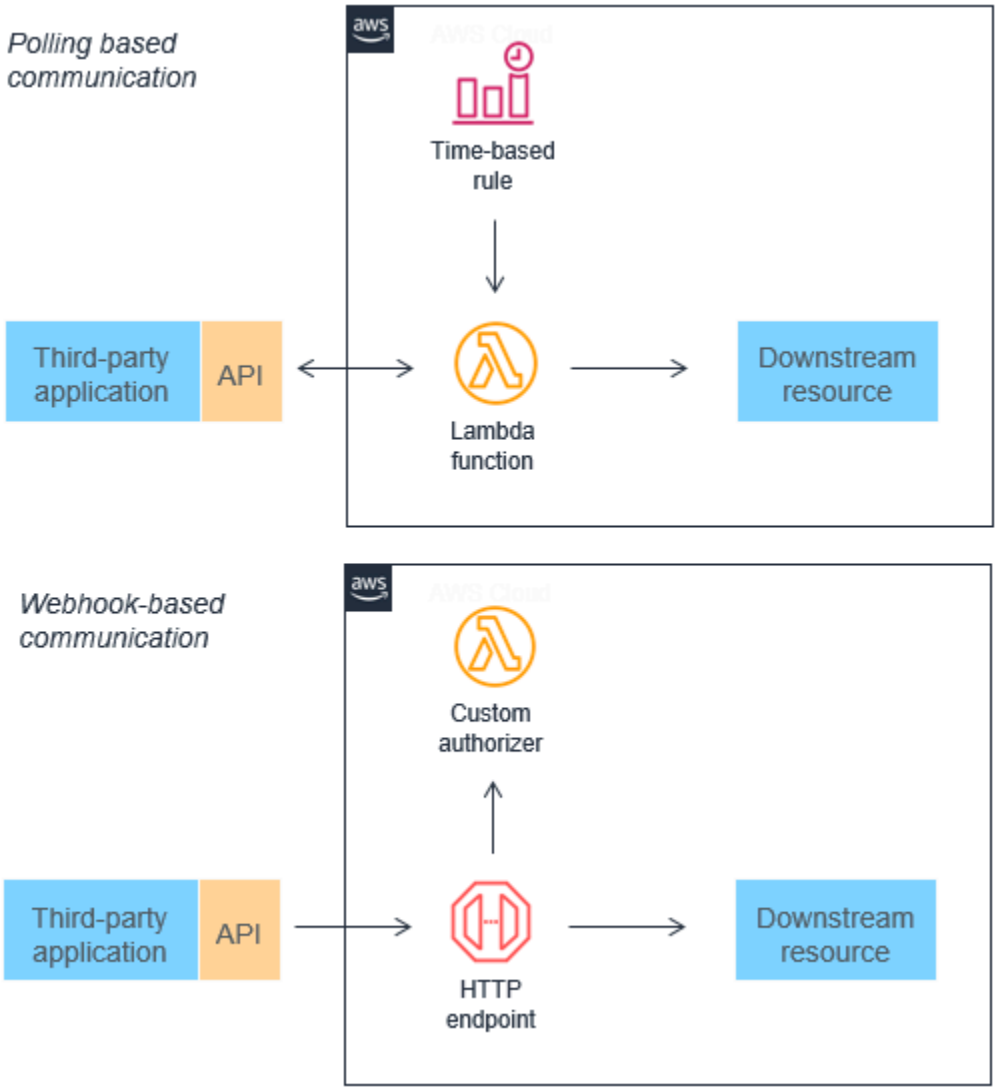
Lambda prend en charge deux méthodes d'invocation dans les architectures pilotées par les événements :

1. Invocation directe (méthode push) : les AWS services déclenchent directement les fonctions Lambda. Par exemple :
   - Amazon S3 déclenche une fonction lorsqu'un fichier est chargé
   - API Gateway déclenche une fonction lors de la réception d'une requête HTTP
2. Mappage des sources d'événements (méthode pull) : Lambda récupère les événements et invoque des fonctions. Par exemple :
   - Lambda récupère les messages d'une file d'attente Amazon SQS et invoque une fonction
   - Lambda lit les enregistrements d'un flux DynamoDB et invoque une fonction

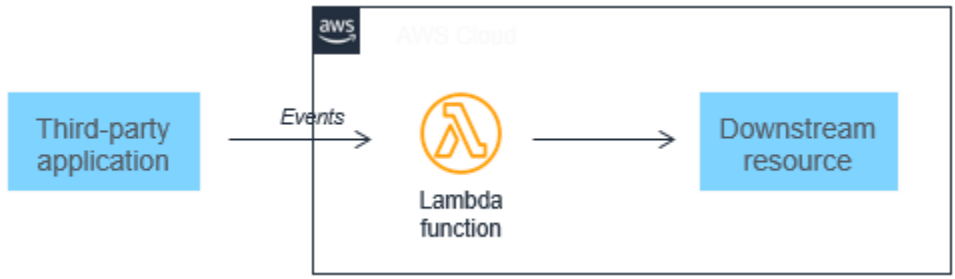
Les deux méthodes contribuent aux avantages des architectures guidées par les événements, comme décrit ci-dessous.

Remplacement des interrogations et des webhooks par des événements

De nombreuses architectures traditionnelles utilisent des mécanismes d'interrogation et de webhook pour communiquer l'état entre différents composants. L'interrogation peut s'avérer très inefficace pour récupérer les mises à jour, car il existe un décalage entre la mise à disposition des nouvelles données et la synchronisation avec les services en aval. Les webhooks ne sont pas toujours pris en charge par les autres microservices auxquels vous souhaitez vous intégrer. Ils peuvent également nécessiter des configurations d'autorisation et d'authentification personnalisées. Dans les deux cas, il est difficile de mettre à l'échelle ces méthodes d'intégration à la demande sans travail supplémentaire de la part des équipes de développement.



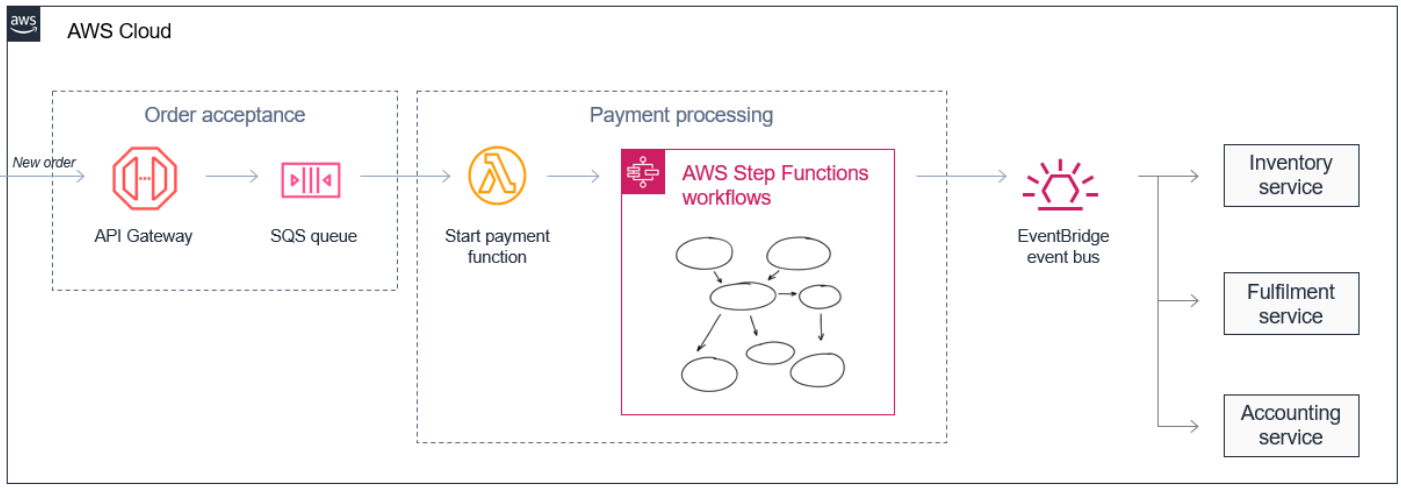
Ces deux mécanismes peuvent être remplacés par des événements, qui peuvent être filtrés, acheminés et redirigés en aval vers les microservices consommateurs. Cette approche peut entraîner une réduction de la consommation de bande passante, de l'utilisation du processeur et potentiellement une baisse des coûts. Ces architectures peuvent également réduire la complexité, étant donné que chaque unité fonctionnelle est plus petite et qu'il y a souvent moins de code.



Event-driven les architectures peuvent également faciliter la conception de systèmes en temps quasi réel, aidant ainsi les entreprises à s'éloigner du traitement par lots. Les événements sont générés au moment où l'état de l'application change. Le code personnalisé d'un microservice doit donc être conçu pour gérer le traitement d'un seul événement. La mise à l'échelle étant gérée par le service Lambda, cette architecture peut gérer des augmentations significatives du trafic sans modifier le code personnalisé. Au fur et à mesure que les événements augmentent verticalement, la couche de calcul qui les traite augmente également.

Réduction de la complexité

Les microservices permettent aux développeurs et aux architectes de simplifier les flux de travail complexes. Par exemple, un monolithe de commerce électronique peut être divisé en processus d'acceptation des commandes et de paiement avec des services d'inventaire, d'exécution et de comptabilité distincts. Ce qui peut s'avérer complexe à gérer et à orchestrer dans un monolithe devient une série de services découplés qui communiquent de manière asynchrone avec les événements.



Cette approche permet également d'assembler des services qui traitent les données à des rythmes différents. Dans ce cas, un microservice d'acceptation des commandes peut stocker de gros volumes de commandes entrantes en mettant les messages en mémoire tampon dans une file d'attente Amazon SQS.

Un service de traitement des paiements, qui est généralement plus lent en raison de la complexité du traitement des paiements, peut recevoir un flux constant de messages provenant de la file d'attente Amazon SQS. Il peut orchestrer une logique complexe de gestion des nouvelles tentatives et des erreurs en utilisant AWS Step Functions et en coordonnant les flux de paiement actifs pour des centaines de milliers de commandes.

Approche alternative : pour l'orchestration à l'aide de langages de programmation standard, vous pouvez utiliser les fonctions durables Lambda. Des fonctions durables vous permettent d'écrire la logique d'acceptation des commandes, de traitement des paiements et de notification dans un code avec pointage automatique et nouvelle tentative. Cette approche fonctionne bien lorsque le flux de travail implique principalement des fonctions Lambda et que vous préférez conserver la logique d'orchestration dans le code.

Amélioration de la capacité de mise à l’échelle et de l’extensibilité

Les microservices génèrent des événements qui sont généralement publiés sur des services de messagerie tels qu’Amazon SNS et Amazon SQS. Ils se comportent comme une mémoire tampon élastique entre les microservices et aident à gérer la mise à l’échelle lorsque le trafic augmente. Des services tels qu'Amazon EventBridge peuvent ensuite filtrer et acheminer les messages en fonction du contenu de l'événement, tel que défini dans les règles. Par conséquent, les applications basées sur les événements peuvent être plus évolutives et offrir une meilleure redondance que les applications monolithiques.

Ce système est également très extensible, ce qui permet aux autres équipes d’étendre les fonctionnalités et d’en ajouter sans affecter les microservices de traitement des commandes et des paiements. En publiant des événements à l'aide de cette application EventBridge, elle s'intègre aux systèmes existants, tels que le microservice d'inventaire, mais permet également à toute future application de s'intégrer en tant que consommateur d'événements. Les producteurs d’événements ne connaissent pas les consommateurs d’événements, ce qui peut contribuer à simplifier la logique des microservices.

Trade-offs d'architectures pilotées par les événements

Latence variable

Contrairement aux applications monolithiques, qui peuvent tout traiter dans le même espace mémoire sur un seul appareil, les applications pilotées par les événements communiquent sur les réseaux. Cette conception introduit une latence variable. Bien qu'il soit possible de concevoir des applications pour minimiser la latence, les applications monolithiques peuvent presque toujours être optimisées pour réduire la latence au détriment de l'évolutivité et de la disponibilité.

Les charges de travail qui nécessitent des performances constantes à faible latence, telles que les applications de négociation à haute fréquence dans les banques ou l’automatisation robotique en moins d’une milliseconde dans les entrepôts, ne sont pas de bonnes candidates pour une architecture guidée par les événements.

Cohérence à terme

Un événement représente un changement d'état, et comme de nombreux événements transitent par différents services d'une architecture à un moment donné, ces charges de travail sont souvent cohérentes à terme. Cela complique le traitement des transactions, la gestion des doublons ou la détermination de l'état global exact d'un système.

Certaines charges de travail contiennent une combinaison d'exigences qui sont cohérentes à terme (par exemple, le nombre total de commandes dans l'heure en cours) ou fortement cohérentes (par exemple, l'inventaire actuel). Pour les charges de travail nécessitant une forte cohérence des données, il existe des modèles d'architecture adaptés. Par exemple :

- DynamoDB peut fournir des lectures fortement cohérentes, parfois avec une latence plus élevée, consommant un débit supérieur à celui du mode par défaut. DynamoDB peut également prendre en charge les transactions afin de garantir la cohérence des données.
- Vous pouvez utiliser Amazon RDS pour les fonctionnalités nécessitant des propriétés ACID, bien que les bases de données relationnelles aient généralement une moins bonne capacité de mise à l'échelle qu'une base de données NoSQL comme DynamoDB. Le Proxy Amazon RDS peut aider à gérer le regroupement et la mise à l'échelle des connexions à partir de clients éphémères tels que les fonctions Lambda.

Event-based les architectures sont généralement conçues en fonction d'événements individuels plutôt que de grands lots de données. En général, les flux de travail sont conçus pour gérer les étapes d'un événement ou d'un flux d'exécution individuel au lieu de traiter plusieurs événements simultanément. En mode sans serveur, le traitement des événements en temps réel est préféré au traitement par lots : les lots doivent être remplacés par de nombreuses mises à jour incrémentales plus petites. Cela peut rendre les charges de travail plus disponibles et évolutives, mais il est également plus difficile pour les événements d'avoir connaissance des autres événements.

Renvoi des valeurs aux appelants

Dans de nombreux cas, les applications basées sur des événements sont asynchrones. Cela signifie que les services des appelants n'attendent pas les requêtes des autres services pour poursuivre d'autres tâches. Il s'agit d'une caractéristique fondamentale des architectures guidées par les événements qui permet la capacité de mise à l'échelle et la flexibilité. Cela signifie que la transmission des valeurs de retour ou du résultat d'un flux de travail est plus complexe que dans les flux d'exécution synchrones.

La plupart des invocations Lambda dans les systèmes de production sont asynchrones et répondent à des événements provenant de services tels qu'Amazon S3 ou Amazon SQS. Dans ces cas, le succès ou l'échec du traitement d'un événement est souvent plus important que le renvoi d'une valeur. Des fonctionnalités telles que les files d'attente de lettres mortes (DLQ) dans Lambda sont fournies pour vous permettre d'identifier et de relancer les événements ayant échoué, sans avoir à en informer l'appelant.

Débogage entre les services et les fonctions

Le débogage de systèmes guidés par des événements est également différent par rapport à une application monolithique. Lorsque différents systèmes et services transmettent des événements, il est impossible d'enregistrer et de reproduire l'état exact de plusieurs services en cas d'erreur. Étant donné que chaque invocation de service et de fonction comporte des fichiers journaux distincts, il peut être plus compliqué de déterminer ce qu'il est advenu d'un événement spécifique à l'origine d'une erreur.

Trois conditions importantes sont requises pour élaborer une approche de débogage réussie dans les systèmes guidés par les événements. Tout d'abord, un système de journalisation robuste est essentiel, fourni par l'ensemble AWS des services et intégré aux fonctions Lambda par Amazon. CloudWatch Deuxièmement, dans ces systèmes, il est important de s'assurer que chaque événement possède un identifiant de transaction enregistré à chaque étape de la transaction, afin de faciliter la recherche de journaux.

Enfin, il est fortement recommandé d'automatiser l'analyse et l'analyse des journaux en utilisant un service de débogage et de surveillance tel que. AWS X-Ray Cela peut consommer les journaux de plusieurs invocations et services Lambda, ce qui permet d'identifier plus facilement la cause racine des problèmes. Reportez-vous à la section Procédure de résolution des problèmes pour une description détaillée de l'utilisation à des X-Ray fins de dépannage.

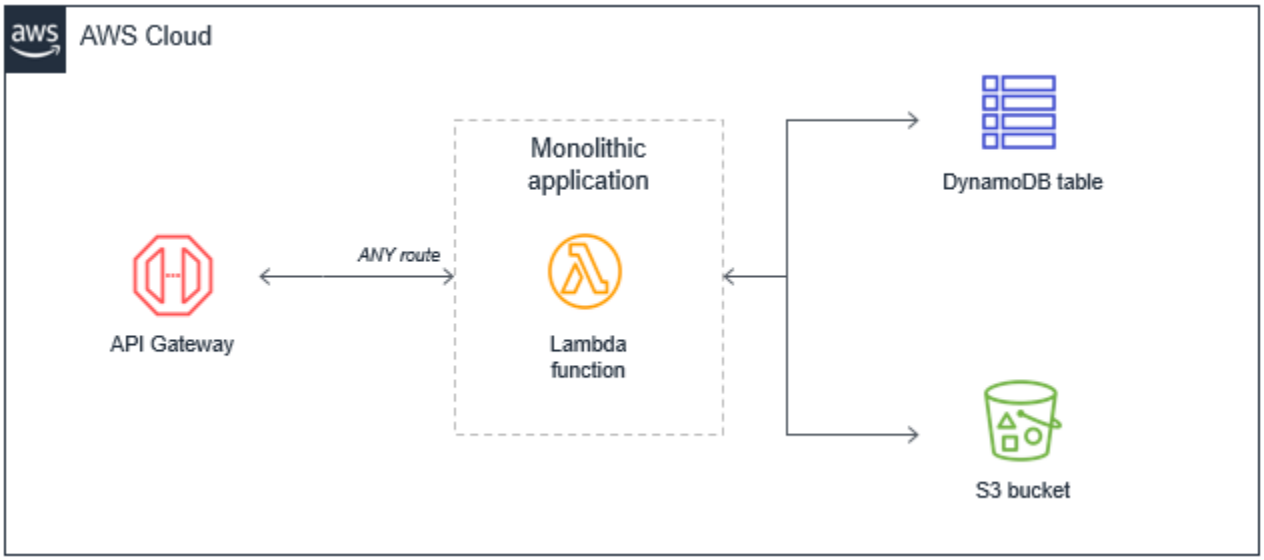
Anti-patterns dans les applications Lambda-based pilotées par les événements

Lorsque vous créez des architectures pilotées par des événements avec Lambda, évitez les anti-modèles courants suivants. Ces modèles fonctionnent mais peuvent augmenter les coûts et la complexité.

Le monolithe Lambda

Dans de nombreuses applications migrées depuis des serveurs traditionnels, telles que les instances Amazon EC2 ou les applications Elastic Beanstalk, les développeurs « modifient et modifient » le code existant. Cela se traduit souvent par une seule fonction Lambda qui contient toute la logique

d’application déclenchée pour tous les événements. Pour une application Web de base, une fonction Lambda monolithique gérerait toutes les routes API Gateway et s’intégrerait à toutes les ressources en aval nécessaires.

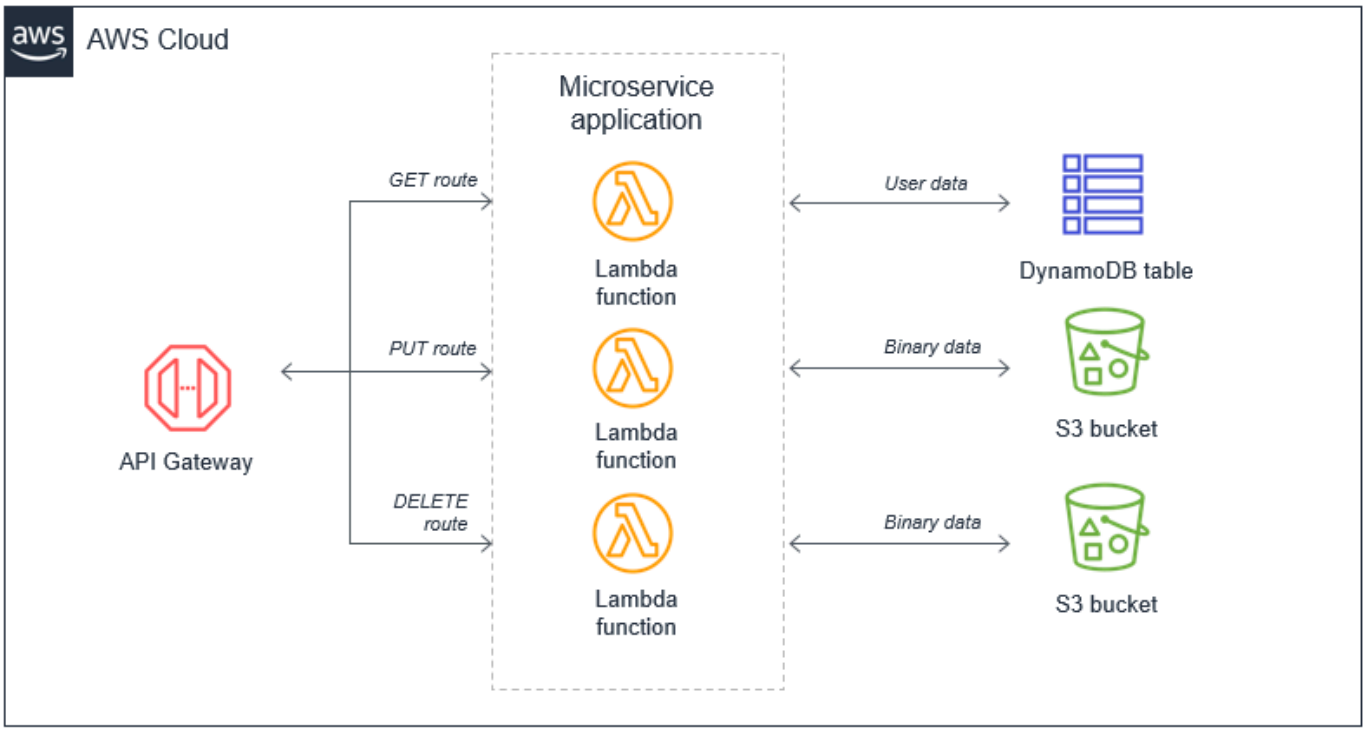


Cette approche présente plusieurs inconvénients :

- Taille du package — La fonction Lambda peut être beaucoup plus importante car elle contient tout le code possible pour tous les chemins, ce qui ralentit l'exécution du service Lambda.
- Difficile d'appliquer le moindre privilège — Le rôle d'exécution de la fonction doit autoriser l'accès à toutes les ressources nécessaires pour tous les chemins, ce qui rend les autorisations très larges. Il s’agit d’un problème de sécurité. De nombreux chemins du monolithe fonctionnel n’ont pas besoin de toutes les autorisations accordées.
- Mise à niveau plus difficile : dans un système de production, toute mise à niveau d’une seule fonction est plus risquée et peut entraîner l’arrêt du fonctionnement de l’application dans son ensemble. La mise à niveau d’un seul chemin dans la fonction Lambda est une mise à niveau de l’ensemble de la fonction.
- Plus difficile à maintenir — Il est plus difficile d'avoir plusieurs développeurs travaillant sur le service puisqu'il s'agit d'un référentiel de code monolithique. Cela alourdit également la charge cognitive des développeurs et complique la création d’une couverture de test appropriée pour le code.
- Réutilisation du code plus difficile : il est plus difficile de séparer les bibliothèques réutilisables des monolithes, ce qui complique la réutilisation du code. Au fur et à mesure que vous développez et soutenez de plus en plus de projets, il peut être plus difficile de soutenir le code et d'augmenter la vitesse de votre équipe.

- Tests plus difficiles : à mesure que le nombre de lignes de code augmente, il devient plus difficile d'effectuer des tests unitaires pour toutes les combinaisons possibles d'entrées et de points d'entrée dans la base de code. Il est généralement plus facile de mettre en œuvre des tests unitaires pour les petits services avec moins de code.

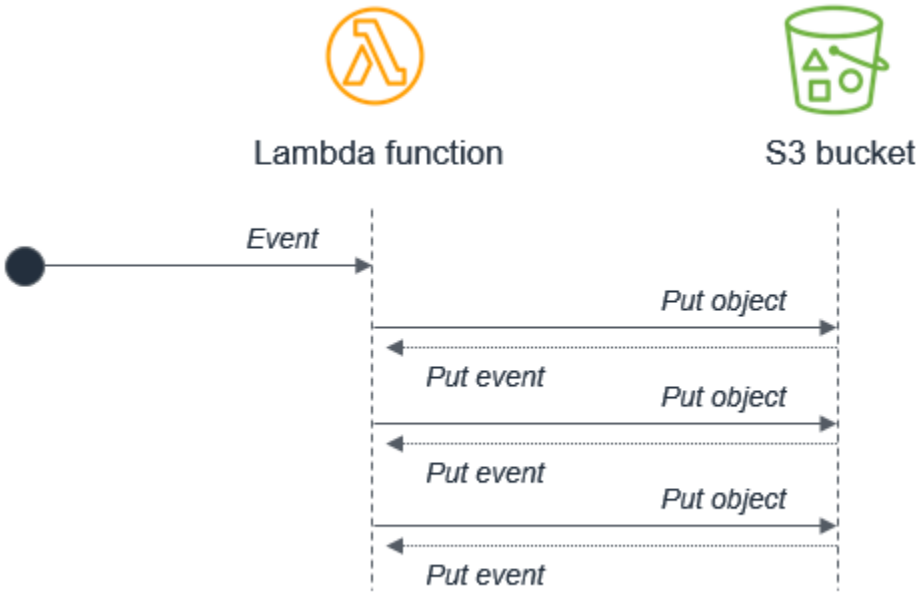
L'alternative préférée consiste à décomposer la fonction Lambda monolithique en microservices individuels, en mappant une seule fonction Lambda à une seule tâche bien définie. Dans cette application Web simple dotée de quelques points de terminaison d'API, l'architecture basée sur les microservices qui en résulte peut être basée sur les routes API Gateway.



Modèles récursifs qui provoquent des fonctions Lambda incontrôlables

AWS les services génèrent des événements qui invoquent des fonctions Lambda, et les fonctions Lambda peuvent envoyer des messages aux services. AWS En général, le service ou la ressource qui invoque une fonction Lambda doit être différent du service ou de la ressource vers lequel la fonction émet des sorties. Si vous ne parvenez pas à gérer cela, vous risquez de créer des boucles infinies.

Par exemple, une fonction Lambda écrit un objet dans un objet Amazon S3, qui à son tour invoque la même fonction Lambda à l'aide d'un événement put. L'invocation entraîne l'écriture d'un deuxième objet dans le compartiment, qui invoque la même fonction Lambda :



Bien que le potentiel de boucles infinies existe dans la plupart des langages de programmation, cet anti-modèle est susceptible de consommer davantage de ressources dans les applications sans serveur. Lambda et Amazon S3 évoluent automatiquement en fonction du trafic, de sorte que la boucle peut amener Lambda à évoluer pour utiliser toute la simultanéité disponible et Amazon S3 continue d'écrire des objets et de générer davantage d'événements pour Lambda.

Cet exemple utilise S3, mais le risque de boucles récursives existe également dans Amazon SNS, Amazon SQS, DynamoDB et d'autres services. Vous pouvez utiliser la détection de boucle récursive pour détecter et éviter cet anti-modèle.

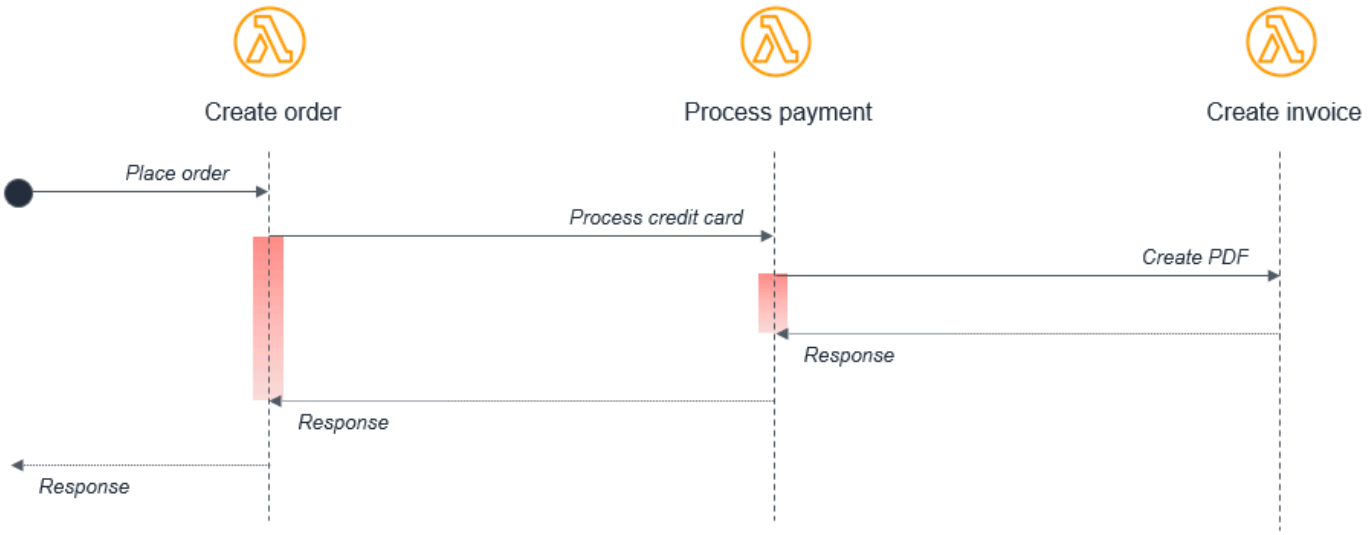
Fonctions Lambda appelant des fonctions Lambda

Les fonctions permettent l'encapsulation et la réutilisation du code. La plupart des langages de programmation prennent en charge le concept d'appel synchrone de fonctions au sein d'une base de code. Dans ce cas, l'appelant attend la réponse de la fonction.

> **Note**
>
> Bien que les fonctions Lambda appelant directement d'autres fonctions Lambda constituent généralement un anti-modèle en raison de problèmes de coût et de complexité, cela ne s'applique pas aux fonctions durables, qui sont spécifiquement conçues pour orchestrer des flux de travail en plusieurs étapes en invoquant d'autres fonctions.

Lorsque cela se produit sur un serveur traditionnel ou une instance virtuelle, le planificateur du système d'exploitation passe à d'autres tâches disponibles. Le fait que le processeur fonctionne à 0 % ou à 100 % n'a aucune incidence sur le coût global de l'application, puisque vous payez le coût fixe lié à la possession et à l'exploitation d'un serveur.

Ce modèle ne s'adapte souvent pas bien au développement sans serveur. Prenons l'exemple d'une simple application de commerce électronique composée de trois fonctions Lambda qui traitent une commande :



Dans ce cas, la fonction Créer une commande appelle la fonction Traiter le paiement, qui à son tour appelle la fonction Créer une facture. Bien que ce flux synchrone puisse fonctionner au sein d'une seule application sur un serveur, il introduit plusieurs problèmes évitables dans une architecture sans serveur distribuée :

- Coût : avec Lambda, vous payez pour la durée d'une invocation. Dans cet exemple, pendant que les fonctions Créer une facture s'exécutent, deux autres fonctions sont également exécutées en attente, comme indiqué en rouge sur le diagramme.
- Gestion des erreurs : dans les invocations imbriquées, la gestion des erreurs peut devenir beaucoup plus complexe. Par exemple, une erreur dans Créer une facture peut nécessiter que la fonction de traitement du paiement annule le débit, ou qu'elle réessaie le processus de création de facture.
- Couplage fort : le traitement d'un paiement prend généralement plus de temps que la création d'une facture. Dans ce modèle, la disponibilité de l'ensemble du flux de travail est limitée par la fonction la plus lente.

- Mise à l'échelle : la simultanéité des trois fonctions doit être égale. Dans un système occupé, cela utilise plus de simultanéité que ce qui serait nécessaire autrement.

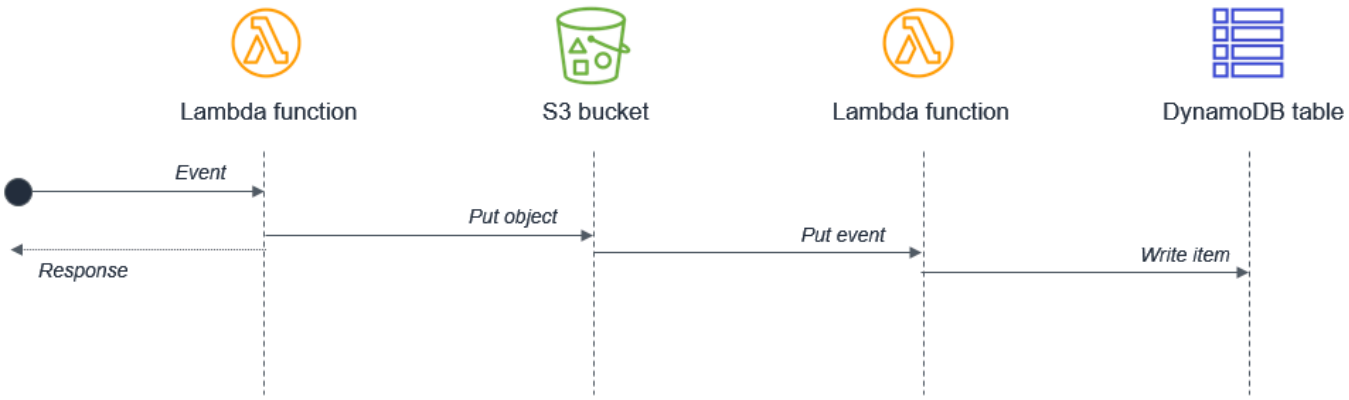
Dans les applications sans serveur, il existe deux approches courantes pour éviter ce schéma. Tout d'abord, utilisez une file d'attente Amazon SQS entre les fonctions Lambda. Si un processus en aval est plus lent qu'un processus en amont, la file d'attente conserve les messages de manière durable et dissocie les deux fonctions. Dans cet exemple, la fonction Create order publierait un message dans une file d'attente Amazon SQS, et la fonction Process payment consomme les messages de la file d'attente.

La deuxième approche consiste à utiliser AWS Step Functions. Pour les processus complexes présentant plusieurs types d'échec et une logique de nouvelle tentative, Step Functions peut aider à réduire la quantité de code personnalisé nécessaire pour orchestrer le flux de travail. Par conséquent, Step Functions orchestre les tâches et gère efficacement les erreurs et les nouvelles tentatives, et les fonctions Lambda ne contiennent que de la logique métier.

Attente synchrone au sein d'une seule fonction Lambda

Assurez-vous que les activités potentiellement simultanées ne sont pas planifiées de manière synchrone au sein d'une seule fonction Lambda. Par exemple, une fonction Lambda peut écrire dans un compartiment S3, puis dans une table DynamoDB :

Dans cette conception, les temps d'attente sont cumulés, car les activités sont séquentielles. Dans les cas où la deuxième tâche dépend de l'achèvement de la première, vous pouvez peut-être réduire le temps d'attente total et le coût d'exécution en ayant deux fonctions Lambda distinctes :



Dans cette conception, la première fonction Lambda répond immédiatement après avoir placé l'objet dans le compartiment Amazon S3. Le service S3 invoque la deuxième fonction Lambda, qui écrit ensuite des données dans la table DynamoDB. Cette approche réduit le temps d'attente total lors des exécutions de fonctions Lambda.

Conception d’applications Lambda

Une application événementielle bien conçue utilise une combinaison de AWS services et de code personnalisé pour traiter et gérer les demandes et les données. Ce chapitre se concentre sur des Lambda-specific sujets liés à la conception d'applications. Les architectes sans serveur doivent tenir compte de nombreuses considérations importantes lorsqu’ils conçoivent des applications pour des systèmes de production très sollicités.

Bon nombre des pratiques exemplaires applicables au développement de logiciels et aux systèmes distribués s’appliquent également au développement d’applications sans serveur. L’objectif global est de développer des charges de travail qui sont :

- Fiables : offrez à vos utilisateurs finaux un haut niveau de disponibilité. Les services AWS sans serveur sont fiables, car ils sont également conçus pour résister aux défaillances.
- Durables : offrez des options de stockage qui répondent aux besoins de durabilité de votre charge de travail.
- Sécurisées : suivez les pratiques exemplaires et utilisez les outils fournis pour sécuriser l’accès aux charges de travail et limiter le rayon d’impact.
- Performantes : utilisez les ressources informatiques avec efficacité et répondez aux besoins de performance de vos utilisateurs finaux.
- Cost-efficient— conception d'architectures qui évitent des coûts inutiles, qui peuvent évoluer sans dépenses excessives et qui peuvent également être mises hors service sans frais supplémentaires importants.

Les principes de conception suivants peuvent vous aider à créer des charges de travail répondant à ces objectifs. Tous les principes ne s'appliquent peut-être pas à toutes les architectures, mais ils devraient vous guider dans vos décisions générales en matière d'architecture.

Rubriques

- Utilisation de services plutôt que de code personnalisé
- Présentation des niveaux d’abstraction Lambda
- Implémenter l’absence d’état dans les fonctions
- Minimiser le couplage
- Générer des données à la demande plutôt que pour des lots
- Choisissez une option d'orchestration pour les flux de travail complexes

- Implémenter l'idempotence
- Utiliser plusieurs AWS comptes pour la gestion des quotas

Utilisation de services plutôt que de code personnalisé

Les applications sans serveur comprennent généralement plusieurs AWS services, intégrés à du code personnalisé exécuté dans les fonctions Lambda. Lambda peut être intégré à la plupart des AWS services, mais les services les plus couramment utilisés dans les applications sans serveur sont les suivants :

Catégorie	AWS service
Calcul	AWS Lambda
Stockage de données	Amazon S3 Amazon DynamoDB Amazon RDS
API	Amazon API Gateway
Intégration d'applications	Amazon EventBridge Amazon SNS Amazon SQS
Orchestration	Fonctions durables Lambda AWS Step Functions
Données de streaming et analytique	Amazon Data Firehose

> **Note**
>
> De nombreux services sans serveur fournissent la réplication et la prise en charge de plusieurs régions, notamment DynamoDB et Amazon S3. Les fonctions Lambda peuvent être déployées dans plusieurs régions dans le cadre d'un pipeline de déploiement, et API

Gateway peut être configurée pour prendre en charge cette configuration. Consultez cet exemple d'architecture qui montre comment cela peut être réalisé.

Il existe de nombreux modèles courants bien établis dans les architectures distribuées que vous pouvez créer vous-même ou implémenter à l'aide de AWS services. Pour la plupart des clients, le développement de ces modèles à partir de zéro présente peu d'intérêt commercial. Lorsque votre application a besoin de l'un de ces modèles, utilisez le AWS service correspondant :

Modèle	AWS service
File d'attente	Amazon SQS
Bus d'événement	Amazon EventBridge
Publish/subscribe (ventilateur)	Amazon SNS
Orchestration	Fonctions durables Lambda AWS Step Functions
API	Amazon API Gateway
Flux d'événement	Amazon Kinesis

Ces services sont conçus pour s'intégrer à Lambda et vous pouvez utiliser l'infrastructure en tant que code (IaC) pour créer et supprimer des ressources dans les services. Vous pouvez utiliser n'importe lequel de ces services via le AWS SDK sans avoir à installer d'applications ou à configurer des serveurs. Maîtriser l'utilisation de ces services par le biais du code dans vos fonctions Lambda est une étape importante pour produire des applications sans serveur bien conçues.

Présentation des niveaux d'abstraction Lambda

Le service Lambda limite votre accès aux systèmes d'exploitation, aux hyperviseurs et au matériel sous-jacents qui exécutent vos fonctions Lambda. Le service améliore et modifie continuellement l'infrastructure afin d'ajouter des fonctionnalités, de réduire les coûts et de rendre le service plus performant. Votre code ne doit émettre aucune hypothèse quant à l'architecture de Lambda et à l'affinité matérielle.

De même, les intégrations de Lambda avec d'autres services sont gérées par AWS, et seul un petit nombre d'options de configuration vous sont proposées. Par exemple, quand API Gateway et Lambda interagissent, il n'y a aucun concept d'équilibrage de charge, puisqu'il est entièrement géré par les services. Vous n'avez également aucun contrôle direct sur les zones de disponibilité utilisées par les services lorsqu'ils invoquent des fonctions à tout moment, ni sur la manière dont Lambda détermine quand réduire ou augmenter verticalement le nombre d'environnements d'exécution.

Cette abstraction vous aide à vous concentrer sur les aspects d'intégration de votre application, le flux de données et la logique métier dans laquelle votre charge de travail apporte de la valeur à vos utilisateurs finaux. En permettant aux services de gérer les mécanismes sous-jacents, vous pouvez développer des applications plus rapidement avec moins de code personnalisé à gérer.

Implémenter l'absence d'état dans les fonctions

Pour les fonctions Lambda, vous devez partir du principe que l'environnement n'existe que pour un seul appel. La fonction doit initialiser tout état requis lors de son premier démarrage. Par exemple, votre fonction peut nécessiter l'extraction de données depuis une table DynamoDB. Elle doit valider toute modification permanente des données sur un magasin durable tel qu'Amazon S3, DynamoDB ou Amazon SQS avant de quitter. Elle ne doit pas s'appuyer sur des structures de données ou des fichiers temporaires existants, ni sur un état interne qui serait géré par de multiples invocations.

Pour initialiser les connexions aux bases de données et les bibliothèques, ou pour initialiser l'état de chargement, vous pouvez tirer parti de l'initialisation statique. Les environnements d'exécution étant réutilisés dans la mesure du possible pour améliorer les performances, vous pouvez amortir le temps nécessaire à l'initialisation de ces ressources sur plusieurs invocations. Cependant, vous ne devez stocker aucune variable ou donnée utilisée dans la fonction dans cette portée globale.

Minimiser le couplage

La plupart des architectures devraient préférer les fonctions plus nombreuses et plus petites aux fonctions moins nombreuses et plus grandes. Le but de chaque fonction doit être de gérer l'événement transmis à la fonction, sans aucune connaissance ni attente quant au flux de travail global ou au volume des transactions. Cela rend la fonction indépendante de la source de l'événement avec un couplage minimal avec les autres services.

Toutes les constantes de portée globale qui changent rarement doivent être implémentées en tant que variables d'environnement afin de permettre les mises à jour sans déploiement. Tous les secrets ou informations sensibles doivent être stockés dans AWS Systems Manager Parameter Store ou dans AWS Secrets Manager et chargés par la fonction. Comme ces ressources sont propres à

un compte, vous pouvez créer des pipelines de génération sur plusieurs comptes. Les pipelines chargent les secrets appropriés par environnement, sans les exposer aux développeurs ni nécessiter de modification du code.

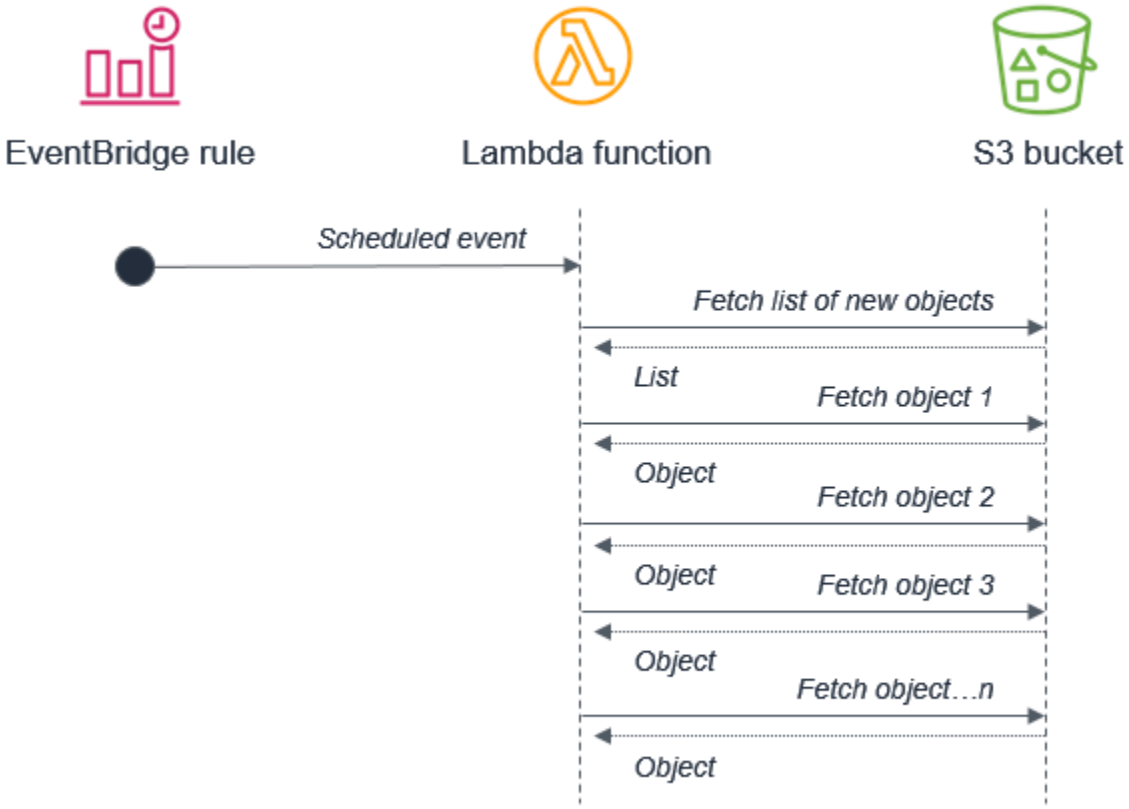
Générer des données à la demande plutôt que pour des lots

De nombreux systèmes traditionnels sont conçus pour fonctionner périodiquement et traiter des lots de transactions accumulés au fil du temps. Par exemple, une application bancaire peut s'exécuter toutes les heures pour traiter les transactions des guichets automatiques dans des registres centraux. Dans Lambda-based les applications, le traitement personnalisé doit être déclenché par chaque événement, ce qui permet au service d'augmenter la simultanéité selon les besoins, afin de fournir un traitement des transactions en temps quasi réel.

Par défaut, l'invocation d'une fonction peut durer jusqu'à 15 minutes. Sur les instances gérées Lambda, les appels asynchrones et de mappage des sources d'événements (ESM) peuvent être exécutés pendant 90 minutes maximum. Pour un traitement plus long, les fonctions durables progressent entre plusieurs invocations. Lorsqu'elle est invoquée de manière asynchrone, une exécution durable peut durer jusqu'à un an. Cependant, vous devez toujours préférer le traitement piloté par les événements au traitement par lots lorsque cela est possible.

Bien que vous puissiez exécuter des tâches cron dans des applications sans serveur en utilisant des expressions planifiées pour les règles dans Amazon EventBridge, celles-ci doivent être utilisées avec parcimonie ou en dernier recours. Dans toute tâche planifiée traitant un lot, il est possible que le volume de transactions augmente au-delà de ce qui peut être traité dans la limite de durée Lambda. Si les limites des systèmes externes vous obligent à utiliser un planificateur, vous devez généralement planifier pour la période récurrente la plus courte possible.

Par exemple, il n'est pas recommandé d'utiliser un processus par lots qui déclenche une fonction Lambda pour récupérer une liste de nouveaux objets Amazon S3. Cela est dû au fait que le service peut recevoir plus de nouveaux objets entre les lots que ce qui peut être traité dans le délai Lambda.



Amazon S3 doit plutôt invoquer la fonction Lambda chaque fois qu'un nouvel objet est placé dans le compartiment. Cette démarche est bien plus facile à mettre à l'échelle et fonctionne en temps quasi réel.

Choisissez une option d'orchestration pour les flux de travail complexes

Les flux de travail qui impliquent une logique de ramification, différents types de modèles d'échec et une logique de nouvelle tentative utilisent généralement un orchestrateur pour suivre l'état de l'exécution globale. Ne créez pas d'orchestration ad hoc dans les fonctions Lambda. Cela entraîne un couplage étroit, un code de routage complexe et aucune restauration automatique de l'état.

Utilisez plutôt l'une de ces options d'orchestration spécialement conçues :

- Fonctions Lambda durables : Application-centric orchestration à l'aide de langages de programmation standard avec point de contrôle automatique, nouvelle tentative intégrée et reprise de l'exécution. Idéal pour les développeurs qui préfèrent conserver la logique du flux de travail dans le code aux côtés de la logique métier dans Lambda.
- AWS Step Functions: orchestration visuelle du flux de travail avec intégrations natives à plus de 220 AWS services. Idéal pour la coordination multiservices, les infrastructures sans maintenance et la conception visuelle des flux de travail.

Pour savoir comment choisir entre ces options, voir Durable functions ou Step Functions.

Avec Step Functions, vous utilisez des machines d'état pour gérer l'orchestration. Cela extrait la logique de gestion des erreurs, de routage et de branchement de votre code, en la remplaçant par des machines d'état déclarées à l'aide de JSON. En plus de rendre les flux de travail plus robustes et observables, vous pouvez également ajouter la gestion des versions aux flux de travail et faire de la machine d'état une ressource codifiée que vous pouvez ajouter à un référentiel de code.

Il est courant que les flux de travail simplifiés dans les fonctions Lambda se complexifient au fil du temps. Lorsque vous utilisez une application de production sans serveur, il est important d'identifier le moment où cela se produit, afin de pouvoir migrer cette logique vers une machine à états ou une fonction durable.

Implémenter l'idempotence

AWS les services sans serveur, y compris Lambda, sont tolérants aux pannes et conçus pour gérer les défaillances. Par exemple, si un service invoque une fonction Lambda et qu'il y a une interruption de service, Lambda invoque votre fonction dans une autre zone de disponibilité. Si la fonction renvoie une erreur, Lambda relance l'invocation.

Comme le même événement peut être reçu plusieurs fois, les fonctions doivent être conçues pour être idempotentes. Cela signifie que le fait de recevoir le même événement plusieurs fois ne change pas le résultat au-delà de la première réception de l'événement.

Vous pouvez implémenter l'idempotence dans les fonctions Lambda en utilisant une table DynamoDB pour suivre les identifiants récemment traités afin de déterminer si la transaction a déjà été traitée. La table DynamoDB implémente généralement une valeur de durée de vie (TTL) pour faire expirer les éléments afin de limiter l'espace de stockage utilisé.

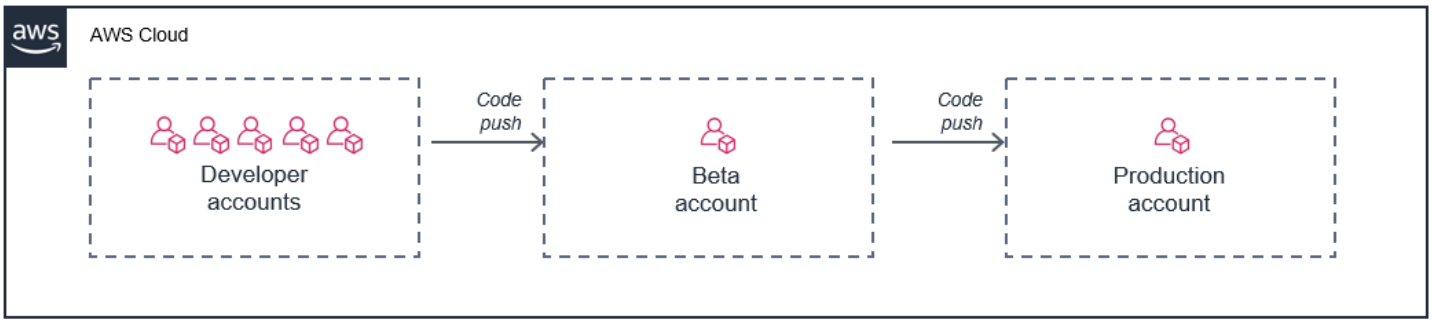
Utiliser plusieurs AWS comptes pour la gestion des quotas

De nombreux quotas de service AWS sont définis au niveau du compte. Cela signifie qu'à mesure que vous ajoutez de nouvelles charges de travail, vous pouvez rapidement épuiser vos limites.

Un moyen efficace de résoudre ce problème consiste à utiliser plusieurs AWS comptes, en consacrant chaque charge de travail à son propre compte. Cela empêche le partage des quotas avec d'autres charges de travail ou des ressources non liées à la production.

Par ailleurs, grâce à AWS Organizations, il est possible de gérer de manière centralisée la facturation, la conformité et la sécurité de ces comptes. Vous pouvez associer des politiques à des groupes de comptes pour éviter les scripts personnalisés et les processus manuels.

Une approche courante consiste à fournir un AWS compte à chaque développeur, puis à utiliser des comptes distincts pour la phase de déploiement et de production de la version bêta :



Dans ce modèle, chaque développeur a son propre ensemble de limites pour le compte, de sorte que leur utilisation n'a aucune incidence sur votre environnement de production. Cette approche permet également aux développeurs de tester les fonctions Lambda localement sur leurs machines de développement par rapport aux ressources cloud actives de leurs comptes individuels.

Création de votre première fonction Lambda

Pour démarrer avec Lambda, utilisez la console Lambda pour créer une fonction. En quelques minutes, vous pouvez créer et déployer une fonction, mais aussi la tester dans la console.

Au cours du didacticiel, vous apprendrez certains concepts fondamentaux de Lambda, tels que la façon de transmettre des arguments à votre fonction à l'aide de l'objet d'événement Lambda. Vous apprendrez également comment renvoyer les sorties de journal de votre fonction et comment consulter les journaux d'invocation de votre fonction sur Amazon CloudWatch Journaux.

Pour simplifier les choses, vous créez votre fonction en utilisant Python ou Node.js exécution. Avec ces langages interprétés, vous pouvez modifier le code de fonction directement dans l'éditeur de code intégré à la console. Avec des langages compilés tels que Java et C#, vous devez créer un package de déploiement sur votre machine de génération locale et le télécharger sur Lambda. Pour en savoir plus sur le déploiement de fonctions sur Lambda à l'aide d'autres environnements d'exécution, consultez les liens figurant dans la section the section called “Étapes suivantes”.

> **Tip**
>
> Pour apprendre à créer des solutions sans serveur, consultez le Guide du développeur sans serveur.

Inscrivez-vous pour Compte AWS

Pour commencer AWS, vous avez besoin d'un Compte AWS. Il existe deux manières de s'inscrire AWS. Si vous souhaitez contrôler totalement la configuration de votre compte et l'emplacement de stockage de votre contenu, ou si vous avez des charges de travail réglementées telles que HIPAA ou FedRAMP, utilisez Inscrivez-vous pour AWS (avancé). Si vous êtes un nouvel utilisateur et que vous souhaitez utiliser un identifiant que vous possédez déjà pour vous connecter AWS et créez un AWS environnement avec des valeurs par défaut préconfigurées dans select Régions AWS, utiliser Inscrivez-vous pour AWS.

Créer une fonction Lambda à l'aide de la console

Dans cet exemple, votre fonction prend un objet JSON contenant deux valeurs entières étiquetées `"length"`et `"width"`. La fonction multiplie ces valeurs pour calculer une zone et la renvoie sous forme de chaîne JSON.

Votre fonction imprime également la zone calculée, ainsi que le nom de sa CloudWatch groupe de journaux. Plus loin dans le didacticiel, vous apprendrez à utiliser CloudWatch Journaux pour consulter les enregistrements de l'invocation de vos fonctions.

Pour créer une fonction Lambda Hello world à l'aide de la console

1. Ouvrez le Page des fonctions de l'événement de la console Lambda.
2. Choisissez Créer une fonction d'événement.
3. Sélectionnez Créer à partir de zéro.
4. Dans le volet Informations de base, pour Nom de la fonction, saisissez **`myLambdaFunction`**.
5. Pour Durée d'exécution, choisissez soit Node.js 24 ou Python 3.14.
6. Partir architecture réglé sur x86_64, puis choisissez Créer une fonction d'événement.

En plus d'une simple fonction qui renvoie le message `Hello from Lambda!`, Lambda crée également un rôle d'exécution pour votre fonction. Un rôle d'exécution est Gestion des identités et des accès AWS Rôle (IAM) qui autorise une fonction Lambda à accéder Services AWS et ressources. Pour votre fonction, le rôle créé par Lambda accorde des autorisations de base pour écrire dans CloudWatch Journaux.

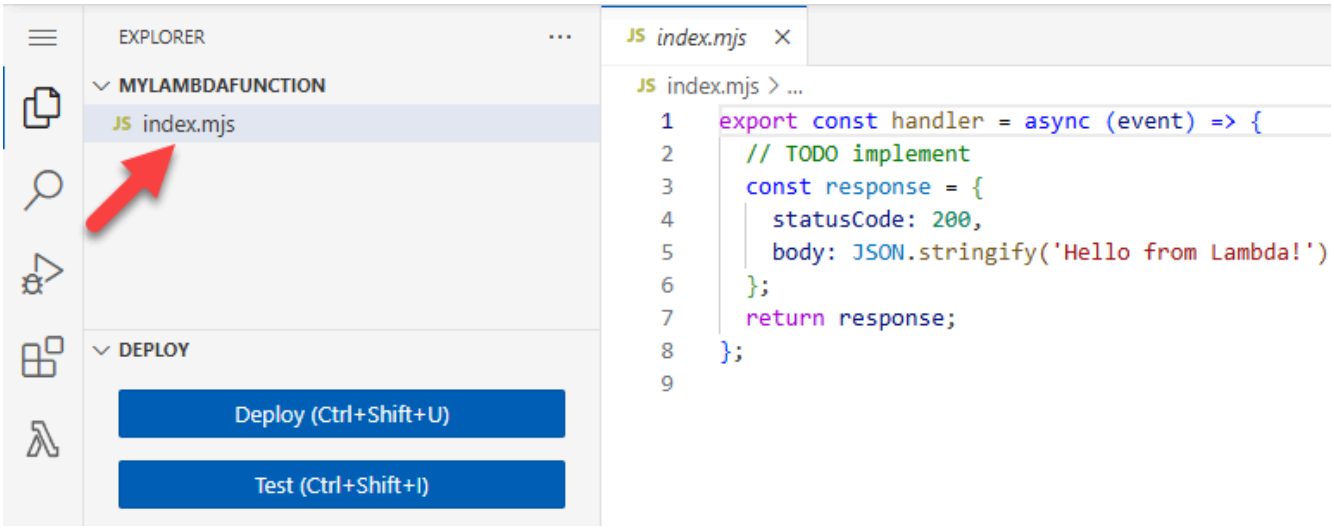
Utilisez l'éditeur de code intégré de la console pour remplacer le code Hello world créé par Lambda avec votre propre code de fonction.

Node.js

Pour modifier le code dans la console

1. Cliquez sur l'onglet Code.

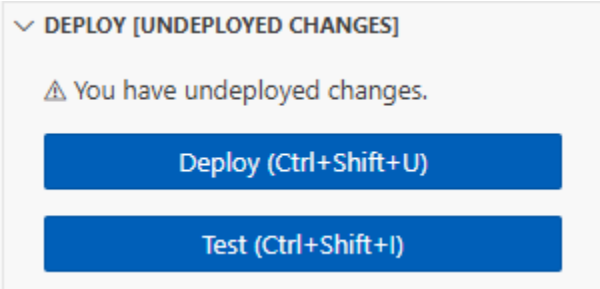
   Dans l'éditeur de code intégré de la console, vous devriez voir le code de fonction créé par Lambda. Si vous ne voyez pas l'onglet index.mjs dans l'éditeur de code, sélectionnez index.mjs dans l'explorateur de fichiers, comme le montre le schéma suivant.



2. Collez le code suivant dans l'onglet index.mjs, en remplaçant le code créé par Lambda.

```
export const handler = async (event, context) => {

  const length = event.length;
  const width = event.width;
  let area = calculateArea(length, width);
  console.log(`The area is ${area}`);

  console.log('CloudWatch log group: ', context.logGroupName);

  let data = {
    "area": area,
  };
    return JSON.stringify(data);

  function calculateArea(length, width) {
    return length * width;
  }
};
```

3. Dans la section DÉPLOYER, choisissez Déployer pour mettre à jour le code de votre fonction :



Comprendre le code de votre fonction

Avant de passer à l'étape suivante, examinons le code de la fonction pour comprendre certains concepts Lambda clés.

- Le gestionnaire Lambda :

  Votre fonction Lambda contient un Node.js fonction nommée `handler`. Une fonction Lambda dans Node.js peut en contenir plus d'un Node.js fonction, mais gestionnaire La fonction est toujours le point d'entrée de votre code. Lorsque votre fonction est invoquée, Lambda exécute cette méthode.

  Lorsque vous avez créé votre fonction Hello world à l'aide de la console, Lambda a automatiquement défini le nom de la méthode du gestionnaire pour votre fonction sur `handler`. Veillez à ne pas modifier le nom de ce Node.js fonction. Si vous le faites, Lambda ne pourra pas exécuter votre code lorsque vous invoquerez votre fonction.

  Pour en savoir plus sur le gestionnaire Lambda dans Node.js, voir the section called “Handler (Gestionnaire)”.
- L'objet de l'événement Lambda :

  La fonction `handler` accepte deux arguments, `event` et `context`. Un événement dans Lambda est un document au format JSON qui contient des données à traiter par votre fonction.

  Si votre fonction est invoquée par un autre Service AWS, l'objet d'événement contient des informations sur l'événement qui a provoqué l'invocation. Par exemple, si votre fonction est invoquée lorsqu’un objet est chargé dans un compartiment Amazon Simple Storage Service (Amazon S3), l’événement contient le nom du compartiment et la clé de l’objet.

  Dans cet exemple, vous allez créer un événement dans la console en saisissant un document au format JSON avec deux paires clé-valeur.

- L'objet de contexte Lambda :

  Le deuxième argument que votre fonction accepte est `context`. Lambda transmet automatiquement l'objet de contexte à votre fonction. L'objet de contexte contient des informations supplémentaires sur l'invocation de la fonction et l'environnement d'exécution.

  Vous pouvez utiliser l'objet de contexte pour générer des informations sur l'invocation de votre fonction à des fins de surveillance. Dans cet exemple, votre fonction utilise le `logGroupName` paramètre pour afficher le nom de son CloudWatch groupe de journaux.

  Pour en savoir plus sur l'objet de contexte Lambda dans Node.js, voir the section called “Contexte”.

- Connexion à Lambda :

  Avec Node.js, vous pouvez utiliser des méthodes de console telles que `console.log` et `console.error` pour envoyer des informations au journal de votre fonction. L'exemple de code utilise `console.log` instructions pour afficher la zone calculée et le nom de la fonction CloudWatch Groupe de journaux. Vous pouvez également utiliser n'importe quelle bibliothèque de journalisation qui écrit dans `stdout` ou `stderr`.

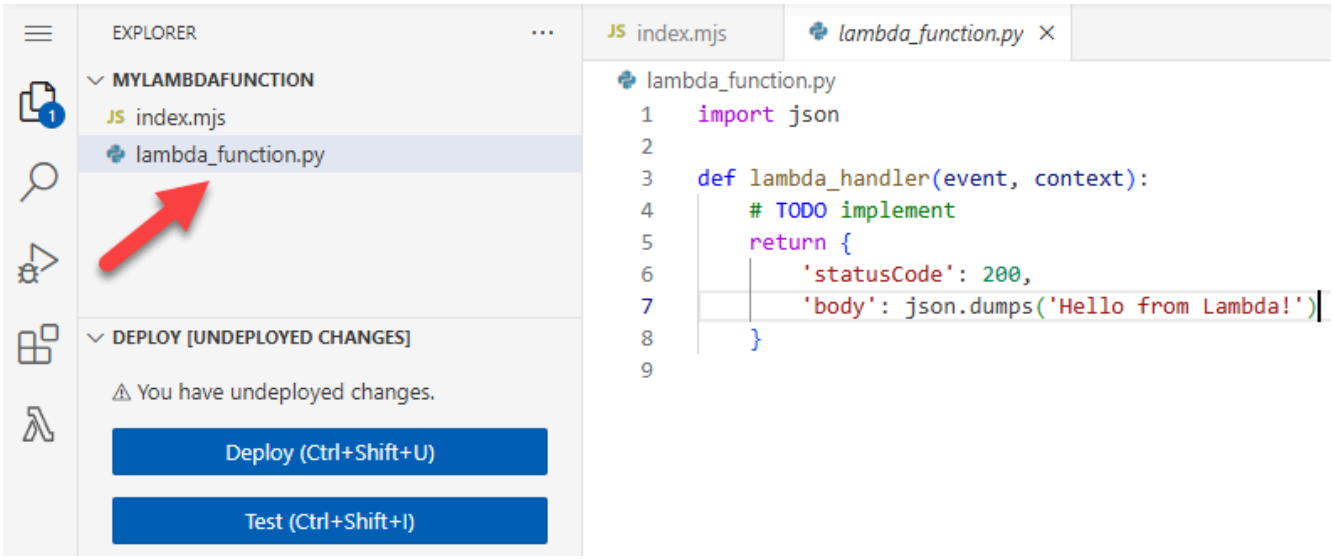
  Pour en savoir plus, consultez the section called “Logging”. Pour en savoir plus sur la connexion à d'autres environnements d'exécution, consultez les pages « Génération avec » correspondant aux environnements d'exécution qui vous intéressent.

Python

Pour modifier le code dans la console

1. Cliquez sur l’onglet Code.

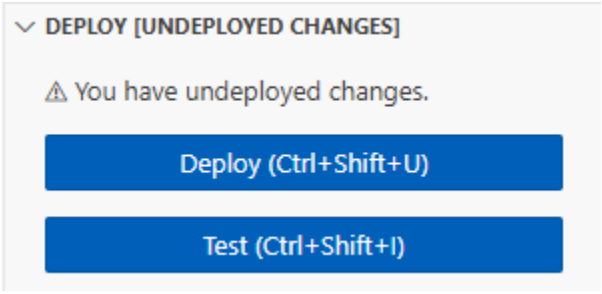
   Dans l'éditeur de code intégré de la console, vous devriez voir le code de fonction créé par Lambda. Si vous ne voyez pas l'onglet lambda_function.py dans l'éditeur de code, sélectionnez lambda_function.py dans l'explorateur de fichiers, comme le montre le schéma suivant.



2. Collez le code suivant dans l'onglet lambda_function.py, en remplaçant le code créé par Lambda.

```
import json
import logging

logger = logging.getLogger()
logger.setLevel(logging.INFO)

def lambda_handler(event, context):

    # Get the length and width parameters from the event object. The
    # runtime converts the event object to a Python dictionary
    length = event['length']
    width = event['width']

    area = calculate_area(length, width)
    print(f"The area is {area}")

    logger.info(f"CloudWatch logs group: {context.log_group_name}")

    # return the calculated area as a JSON string
    data = {"area": area}
    return json.dumps(data)

def calculate_area(length, width):
    return length*width
```

3. Dans la section DÉPLOYER, choisissez Déployer pour mettre à jour le code de votre fonction :



Comprendre le code de votre fonction

Avant de passer à l'étape suivante, examinons le code de la fonction pour comprendre certains concepts Lambda clés.

- Le gestionnaire Lambda :

  Votre fonction Lambda contient une fonction Python nommée `lambda_handler`. Une fonction Lambda en Python peut contenir plusieurs fonctions Python, mais la fonction gestionnaire est toujours le point d'entrée de votre code. Lorsque votre fonction est invoquée, Lambda exécute cette méthode.

  Lorsque vous avez créé votre fonction Hello world à l'aide de la console, Lambda a automatiquement défini le nom de la méthode du gestionnaire pour votre fonction sur `lambda_handler`. Veillez à ne pas modifier le nom de cette fonction Python. Si vous le faites, Lambda ne pourra pas exécuter votre code lorsque vous invoquerez votre fonction.

  Pour en savoir plus sur le gestionnaire Lambda en Python, voir the section called “Handler (Gestionnaire)”.

- L'objet de l'événement Lambda :

  La fonction `lambda_handler` accepte deux arguments, `event` et `context`. Un événement dans Lambda est un document au format JSON qui contient des données à traiter par votre fonction.

  Si votre fonction est invoquée par un autre Service AWS, l'objet d'événement contient des informations sur l'événement qui a provoqué l'invocation. Par exemple, si votre fonction est invoquée lorsqu’un objet est chargé dans un compartiment Amazon Simple Storage Service (Amazon S3), l’événement contient le nom du compartiment et la clé de l’objet.

Dans cet exemple, vous allez créer un événement dans la console en saisissant un document au format JSON avec deux paires clé-valeur.

- L'objet de contexte Lambda :

  Le deuxième argument que votre fonction accepte est `context`. Lambda transmet automatiquement l'objet de contexte à votre fonction. L'objet de contexte contient des informations supplémentaires sur l'invocation de la fonction et l'environnement d'exécution.

  Vous pouvez utiliser l'objet de contexte pour générer des informations sur l'invocation de votre fonction à des fins de surveillance. Dans cet exemple, votre fonction utilise le `log_group_name` paramètre pour afficher le nom de son CloudWatch groupe de journaux.

  Pour en savoir plus sur l'objet de contexte Lambda en Python, voir the section called “Contexte”.

- Connexion à Lambda :

  Avec Python, vous pouvez utiliser une instruction `print` ou une bibliothèque de journalisation Python pour envoyer des informations au journal de votre fonction. Pour illustrer la différence entre ce qui est capturé, l'exemple de code utilise les deux méthodes. Dans une application de production, nous vous recommandons d'utiliser une bibliothèque de journalisation.

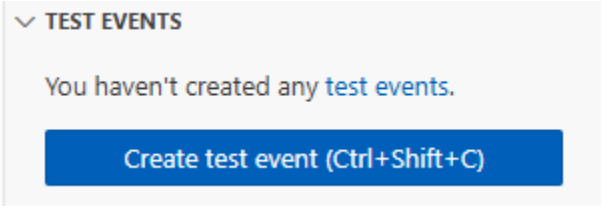
  Pour en savoir plus, consultez the section called “Logging”. Pour en savoir plus sur la connexion à d'autres environnements d'exécution, consultez les pages « Génération avec » correspondant aux environnements d'exécution qui vous intéressent.

Invocation de fonction Lambda à l’aide de l’éditeur de code de la console

Pour invoquer votre fonction à l’aide de l’éditeur de code de la console Lambda, créez un événement de test à envoyer à votre fonction. L'événement est un document au format JSON contenant deux paires clé-valeur avec les clés `"length"` et `"width"`.

Pour créer l'événement de test

1. Dans la section ÉVÉNEMENTS DE TEST de l’éditeur de code de console, choisissez Créer un événement de test.



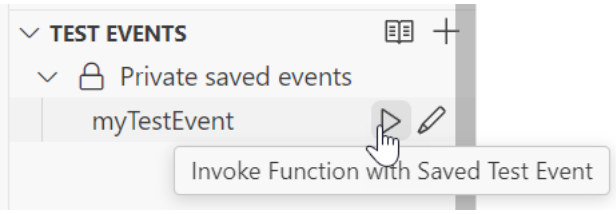
2. Dans Event Name (Nom de l'événement), saisissez **`myTestEvent`**.
3. Dans la section JSON d'événement, remplacez le JSON par défaut par ce qui suit :

```
{
  "length": 6,
  "width": 7
}
```

4. Cliquez sur Enregistrer.

Pour tester votre fonction et consulter les enregistrements d'invocation

Dans la section ÉVÉNEMENTS DE TEST de l'éditeur de code de la console, cliquez sur l'icône d'exécution à côté de votre événement de test :



Lorsque votre fonction termine son exécution, les journaux des réponses et de la fonction s'affichent dans l'onglet RÉSULTATS. Vous devriez voir des résultats similaires à ce qui suit :

Node.js

```
Status: Succeeded
Test Event Name: myTestEvent

Response
"{\"area\":42}"

Function Logs
START RequestId: 5c012b0a-18f7-4805-b2f6-40912935034a Version: $LATEST
2024-08-31T23:39:45.313Z 5c012b0a-18f7-4805-b2f6-40912935034a INFO The area is 42
```

```
2024-08-31T23:39:45.331Z 5c012b0a-18f7-4805-b2f6-40912935034a INFO CloudWatch log
 group:  /aws/lambda/myLambdaFunction
END RequestId: 5c012b0a-18f7-4805-b2f6-40912935034a
REPORT RequestId: 5c012b0a-18f7-4805-b2f6-40912935034a Duration: 20.67 ms Billed
 Duration: 21 ms Memory Size: 128 MB Max Memory Used: 66 MB Init Duration: 163.87 ms

Request ID
5c012b0a-18f7-4805-b2f6-40912935034a
```

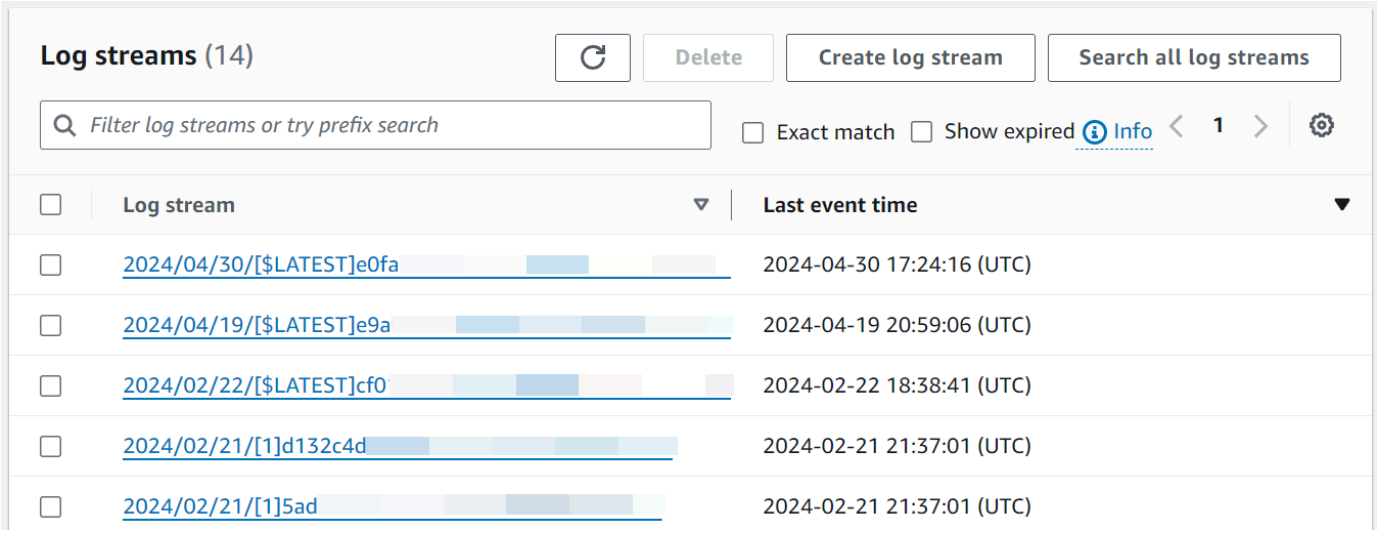
Python

```
Status: Succeeded
Test Event Name: myTestEvent

Response
"{\"area\": 42}"

Function Logs
START RequestId: 2d0b1579-46fb-4bf7-a6e1-8e08840eae5b Version: $LATEST
The area is 42
[INFO] 2024-08-31T23:43:26.428Z 2d0b1579-46fb-4bf7-a6e1-8e08840eae5b CloudWatch logs
 group: /aws/lambda/myLambdaFunction
END RequestId: 2d0b1579-46fb-4bf7-a6e1-8e08840eae5b
REPORT RequestId: 2d0b1579-46fb-4bf7-a6e1-8e08840eae5b Duration: 1.42 ms Billed
 Duration: 2 ms Memory Size: 128 MB Max Memory Used: 39 MB Init Duration: 123.74 ms

Request ID
2d0b1579-46fb-4bf7-a6e1-8e08840eae5b
```

Lorsque vous appelez votre fonction en dehors de la console Lambda, vous devez utiliser CloudWatch Journaux pour afficher les résultats d'exécution de votre fonction.

Pour consulter les enregistrements d'invocation de votre fonction dans CloudWatch Journaux

1. Ouvrez le Groupes de journaux page du CloudWatch console.
2. Choisissez le groupe de journaux de votre fonction (`/aws/lambda/myLambdaFunction`). Il s'agit du nom du groupe de journaux que votre fonction a imprimé sur la console.
3. Faites défiler la page vers le bas et choisissez le flux de journaux pour les invocations de fonctions que vous souhaitez consulter.



Vous devez voir des résultats similaires à ce qui suit :

Node.js

```
INIT_START Runtime Version: nodejs:22.v13    Runtime Version ARN:
 arn:aws:lambda:us-
west-2::runtime:e3aaabf6b92ef8755eaae2f4bfdcb7eb8c4536a5e044900570a42bdba7b869d9
START RequestId: aba6c0fc-cf99-49d7-a77d-26d805dacd20 Version: $LATEST
2024-08-23T22:04:15.809Z    5c012b0a-18f7-4805-b2f6-40912935034a  INFO The area
 is 42
2024-08-23T22:04:15.810Z    aba6c0fc-cf99-49d7-a77d-26d805dacd20  INFO
 CloudWatch log group:  /aws/lambda/myLambdaFunction
END RequestId: aba6c0fc-cf99-49d7-a77d-26d805dacd20
REPORT RequestId: aba6c0fc-cf99-49d7-a77d-26d805dacd20    Duration: 17.77 ms
 Billed Duration: 18 ms    Memory Size: 128 MB    Max Memory Used: 67 MB    Init
 Duration: 178.85 ms
```

Python

```
INIT_START Runtime Version: python:3.13.v16    Runtime Version ARN:
 arn:aws:lambda:us-
west-2::runtime:ca202755c87b9ec2b58856efb7374b4f7b655a0ea3deb1d5acc9aee9e297b072
START RequestId: 9d4096ee-acb3-4c25-be10-8a210f0a9d8e Version: $LATEST
The area is 42
[INFO] 2024-09-01T00:05:22.464Z 9315ab6b-354a-486e-884a-2fb2972b7d84 CloudWatch
 logs group: /aws/lambda/myLambdaFunction
END RequestId: 9d4096ee-acb3-4c25-be10-8a210f0a9d8e
```

```
REPORT RequestId: 9d4096ee-acb3-4c25-be10-8a210f0a9d8e    Duration: 1.15 ms
 Billed Duration: 2 ms    Memory Size: 128 MB    Max Memory Used: 40 MB
```

Nettoyage

Lorsque vous avez terminé d'utiliser l'exemple de fonction, supprimez-le. Vous pouvez également supprimer le groupe de journaux qui stocke les journaux de la fonction, et le rôle d'exécution créé par la console.

Pour supprimer la fonction événementielle Lambda

1. Ouvrez le Page des fonctions de l'événement de la console Lambda.
2. Sélectionnez la fonction d'événement que vous avez créée.
3. Sélectionnez Actions, Supprimer.
4. Saisissez **`confirm`** dans la zone de saisie de texte et choisissez Delete (Supprimer).

Pour supprimer le groupe de journaux

1. Ouvrez la page Log groups (Groupes de journaux) de la console CloudWatch.
2. Sélectionnez le groupe de journaux de la fonction (`/aws/lambda/myLambdaFunction`).
3. Sélectionnez Actions, Delete log group(s) (Supprimer le ou les groupes de journaux).
4. Dans la boîte de dialogue Delete log group(s) (Supprimer le ou les groupes de journaux), sélectionnez Delete (Supprimer).

Pour supprimer le rôle d'exécution

1. Ouvrez le Page des rôles de la Gestion des identités et des accès AWS console (IAM).
2. Sélectionnez le rôle d'exécution de la fonction (par exemple, `myLambdaFunction-role-31exxmpl`).
3. Sélectionnez Supprimer.
4. Dans la fenêtre de dialogue Supprimer le rôle, saisissez le nom du rôle, puis sélectionnez Supprimer.

Ressources supplémentaires et prochaines étapes

Maintenant que vous avez créé et testé une fonction Lambda simple à l'aide de la console, procédez comme suit :

- Découvrez comment ajouter des dépendances à votre fonction et à les déployer à l'aide d'un package de déploiement .zip. Choisissez votre langage préféré à partir des liens suivants.

  Node.js

  the section called “Déploiement d'archives de fichiers .zip”

  Typescript

  the section called “Déployez des archives de fichiers .zip”

  Python

  the section called “Déploiement d'archives de fichiers .zip”

  Ruby

  the section called “Déploiement d'archives de fichiers .zip”

  Java

  the section called “Déploiement d'archives de fichiers .zip”

  Go

  the section called “Déploiement d'archives de fichiers .zip”

  C#

  the section called “Package de déploiement”

- Pour savoir comment invoquer une fonction Lambda à l'aide d'une autre Service AWS, voir Tutoriel : Utilisation d'un déclencheur Amazon S3 pour appeler une fonction d'événement Lambda.
- Choisissez l'un des tutoriels suivants pour un exemple plus complexe d'utilisation de Lambda avec d'autres Services AWS.
  - Didacticiel : Utiliser Lambda avec Amazon API Gateway : créer une API REST Amazon API Gateway qui invoque une fonction Lambda.
  - Utilisation d'une fonction Lambda pour accéder à une base de données Amazon RDS: utilisez une fonction Lambda pour écrire des données dans une base de données Amazon Relational Database Service (Amazon RDS) via un proxy RDS.

- Utilisation d'un déclencheur Amazon S3 pour créer des images miniatures : utilisez une fonction Lambda pour créer une miniature chaque fois qu'un fichier image est chargé dans un compartiment Amazon S3.

Commencer avec des exemples d’applications et de modèles

Les ressources suivantes peuvent être utilisées pour créer et déployer rapidement des applications sans serveur qui mettent en œuvre certains cas d’utilisation courants de Lambda. Pour chacun des exemples d'applications, nous fournissons des instructions pour créer et configurer des ressources manuellement à l'aide de Console de gestion AWS, ou pour les utiliser pour déployer les ressources AWS Serverless Application Model à l'aide d'IaC. Suivez les instructions de la console pour en savoir plus sur la configuration des AWS ressources individuelles pour chaque application, ou utilisez-la pour AWS SAM déployer rapidement des ressources comme vous le feriez dans un environnement de production.

Traitement des fichiers

- Application de chiffrement de PDF : créez une application sans serveur qui chiffre les fichiers PDF lorsqu’ils sont chargés dans un compartiment Amazon Simple Storage Service et les enregistre dans un autre compartiment, ce qui est utile pour sécuriser les documents sensibles lors de leur chargement.

- Application d’analyse d’images : créez une application sans serveur qui extrait le texte des images à l’aide d’Amazon Rekognition, ce qui est utile pour le traitement des documents, la modération de contenu et l’analyse automatique des images.

Intégration de base de données

- Queue-to-Database Application : créez une application sans serveur qui écrit des messages de file d'attente dans une base de données Amazon RDS, ce qui est utile pour traiter les inscriptions des utilisateurs et gérer les soumissions de commandes.

- Gestionnaire d’événements de base de données : créez une application sans serveur qui répond aux modifications des tables Amazon DynamoDB, ce qui est utile pour la journalisation des audits, la réplication des données et les flux de travail automatisés.

Tâches planifiées

- Application de maintenance de base de données : créez une application sans serveur qui supprime automatiquement les entrées datant de plus de 12 mois d'une table Amazon DynamoDB selon un calendrier cron. Ceci est utile pour la maintenance automatisée des bases de données et la gestion du cycle de vie des données.
- Créez un EventBridge calendrier de planification pour les fonctions Lambda : utilisez le EventBridge planificateur pour appeler une fonction Lambda selon un calendrier ponctuel ou récurrent. EventBridge Scheduler prend en charge les expressions cron et rate, les fenêtres horaires flexibles, les politiques de nouvelle tentative et les files d'attente avec lettres mortes. Vous pouvez créer un planning directement depuis la console Lambda à l'aide du flux de déclenchement Add, ou depuis la console EventBridge Scheduler.

Ressources supplémentaires

Utilisez les ressources suivantes pour explorer plus en détail le développement d’applications Lambda et sans serveur :

- Serverless Land : une bibliothèque de modèles prêts à l’emploi pour créer des applications sans serveur. Il aide les développeurs à créer des applications plus rapidement à l'aide de AWS services tels que Lambda, API Gateway et EventBridge. Le site propose des solutions prédéfinies et des bonnes pratiques, afin de faciliter le développement de systèmes sans serveur.
- Exemples d'applications Lambda : applications disponibles dans le GitHub référentiel de ce guide. Ces exemples illustrent l'utilisation de différentes langues et de différents AWS services. Chaque exemple d’application comprend des scripts facilitant le déploiement et le nettoyage, ainsi que des ressources complémentaires.
- Exemples de code pour Lambda à l'aide de kits de développement logiciel (AWS SDK) : exemples qui vous montrent comment utiliser Lambda avec des kits de développement AWS logiciel (SDK). Ces exemples incluent les notions de base, les actions, les scénarios et les contributions de AWS la communauté. Les exemples couvrent les opérations essentielles, les fonctions de service individuelles et les tâches spécifiques utilisant plusieurs fonctions ou AWS services.

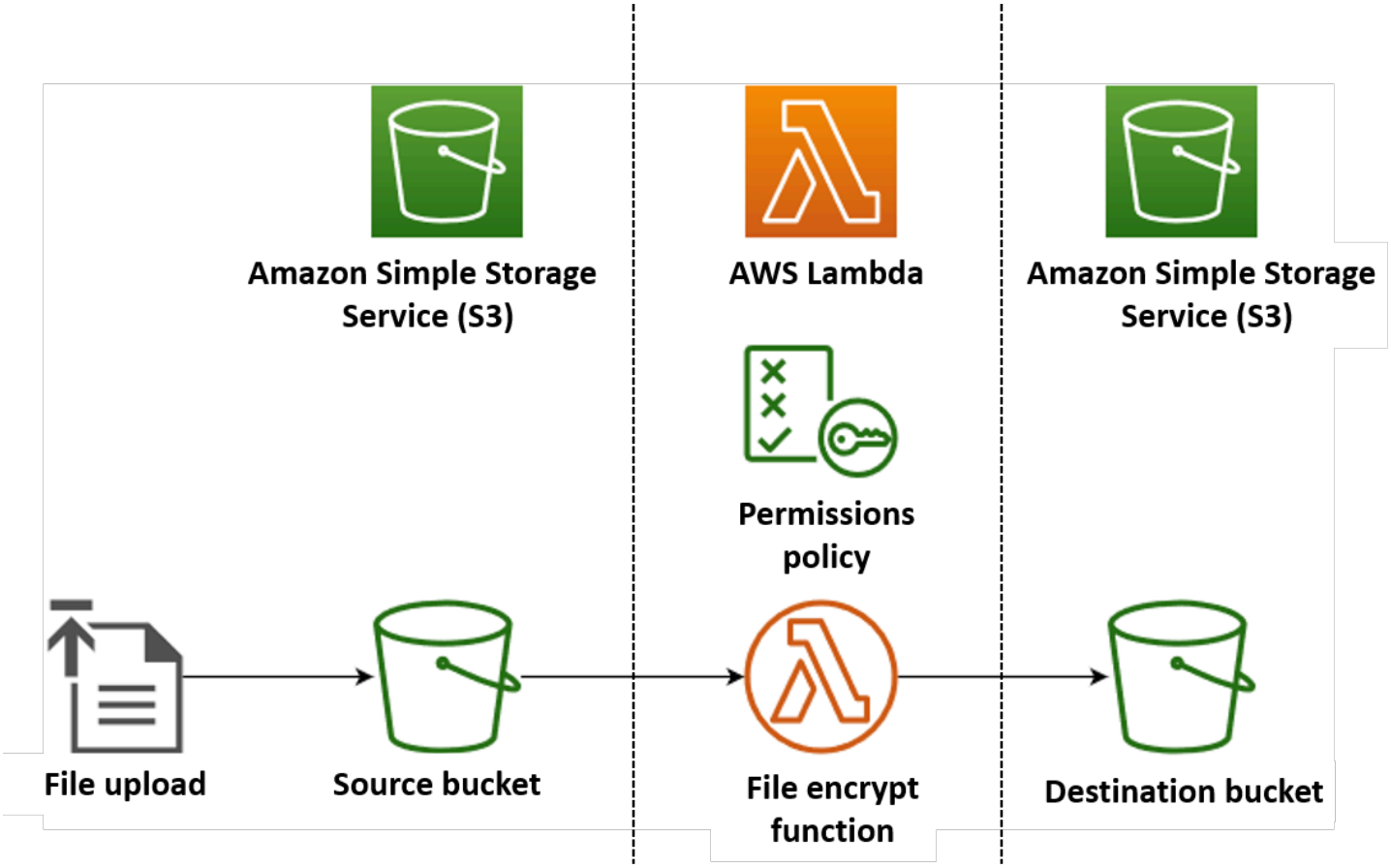
Création d’une application sans serveur de traitement de fichiers

L’un des cas d’utilisation les plus courants de Lambda consiste à effectuer des tâches de traitement de fichiers. Par exemple, vous pouvez utiliser une fonction Lambda pour créer automatiquement des fichiers PDF à partir de fichiers HTML ou d’images, ou pour créer des miniatures lorsqu’un utilisateur télécharge une image.

Dans cet exemple, vous créez une application qui chiffre automatiquement les fichiers PDF lorsqu’ils sont chargés dans un compartiment Amazon Simple Storage Service (Amazon S3). Pour mettre en œuvre cette application, vous créez les ressources suivantes :

- Un compartiment S3 dans lequel les utilisateurs peuvent charger des fichiers PDF
- Une fonction Lambda en Python qui lit le fichier téléchargé et en crée une version cryptée et protégée par mot de passe
- Un deuxième compartiment S3 dans lequel Lambda pourra enregistrer le fichier chiffré

Vous créez également une politique Gestion des identités et des accès AWS (IAM) pour autoriser votre fonction Lambda à effectuer des opérations de lecture et d'écriture sur vos compartiments S3.



> **Tip**
>
> Si vous utilisez Lambda pour la première fois, nous vous recommandons de commencer par le didacticiel the section called “Création de votre première fonction” avant de créer cet exemple d'application.

Vous pouvez déployer votre application manuellement en créant et en configurant des ressources à l'aide du Console de gestion AWS ou du AWS Command Line Interface (AWS CLI). Vous pouvez également déployer l'application en utilisant le AWS Serverless Application Model (AWS SAM). AWS SAM est un outil d'infrastructure en tant que code (IaC). Avec IaC, vous ne créez pas de ressources manuellement, mais vous les définissez dans le code, puis vous les déployez automatiquement.

Si vous souhaitez en savoir plus sur l’utilisation de Lambda avec l’IaC avant de déployer cet exemple d’application, consultez the section called “Infrastructure en tant que code (IaC)”.

Créer les fichiers de code source de la fonction Lambda

Créez les fichiers suivants dans le répertoire de votre projet :

- `lambda_function.py` : le code de fonction Python de la fonction Lambda qui effectue le chiffrement de fichiers
- `requirements.txt` : un fichier manifeste définissant les dépendances requises par le code de votre fonction Python

Développez les sections suivantes pour afficher le code et pour en savoir plus sur le rôle de chaque fichier. Pour créer les fichiers sur votre machine locale, copiez et collez le code ci-dessous ou téléchargez les fichiers depuis le dépôt GitHub aws-lambda-developer-guide.

Code de fonction Python

Copiez et collez le code suivant dans un fichier nommé `lambda_function.py`.

```
from pypdf import PdfReader, PdfWriter
import uuid
import os
from urllib.parse import unquote_plus
import boto3

# Create the S3 client to download and upload objects from S3
s3_client = boto3.client('s3')

def lambda_handler(event, context):
    # Iterate over the S3 event object and get the key for all uploaded files
    for record in event['Records']:
        bucket = record['s3']['bucket']['name']
        key = unquote_plus(record['s3']['object']['key']) # Decode the S3 object key to
 remove any URL-encoded characters
        download_path = f'/tmp/{uuid.uuid4()}.pdf' # Create a path in the Lambda tmp
 directory to save the file to
        upload_path = f'/tmp/converted-{uuid.uuid4()}.pdf' # Create another path to
 save the encrypted file to

        # If the file is a PDF, encrypt it and upload it to the destination S3 bucket
        if key.lower().endswith('.pdf'):
            s3_client.download_file(bucket, key, download_path)
            encrypt_pdf(download_path, upload_path)
            encrypted_key = add_encrypted_suffix(key)
```

```
            s3_client.upload_file(upload_path, f'{bucket}-encrypted', encrypted_key)

# Define the function to encrypt the PDF file with a password
def encrypt_pdf(file_path, encrypted_file_path):
    reader = PdfReader(file_path)
    writer = PdfWriter()

    for page in reader.pages:
        writer.add_page(page)

    # Add a password to the new PDF
    writer.encrypt("my-secret-password")

    # Save the new PDF to a file
    with open(encrypted_file_path, "wb") as file:
        writer.write(file)

# Define a function to add a suffix to the original filename after encryption
def add_encrypted_suffix(original_key):
    filename, extension = original_key.rsplit('.', 1)
    return f'{filename}_encrypted.{extension}'
```

> **Note**
>
> Dans cet exemple de code, un mot de passe pour le fichier chiffré (`my-secret-password`) est codé en dur dans le code de fonction. Dans une application de production, n'incluez pas d'informations sensibles telles que des mots de passe dans votre code de fonction. Créez plutôt un AWS Secrets Manager secret, puis utilisez l'extension Lambda AWS Parameters and Secrets pour récupérer vos informations d'identification dans votre fonction d'événement Lambda.

Le code de la fonction python contient trois fonctions : la fonction de gestion que Lambda exécute lorsque votre fonction est invoquée, et deux fonctions distinctes nommées `add_encrypted_suffix` et `encrypt_pdf` que le gestionnaire appelle pour effectuer le chiffrement du PDF.

Lorsque votre fonction est invoquée par Amazon S3, Lambda transmet un argument d'événement au format JSON à la fonction contenant des informations sur l'événement à l'origine de l'invocation. Dans ce cas, les informations incluent le nom du compartiment S3 et les clés d'objet pour les fichiers téléchargés. Pour de plus amples informations sur le format de l'objet d'événement pour Amazon S3, consultez the section called "S3".

Votre fonction utilise ensuite le AWS SDK pour Python (Boto3) pour télécharger les fichiers PDF spécifiés dans l'objet d'événement vers son répertoire de stockage temporaire local, avant de les chiffrer à l'aide de la bibliothèque pypdf.

Enfin, la fonction utilise le kit SDK Boto3 pour stocker le fichier chiffré dans votre compartiment de destination S3.

`fichier manifeste requirements.txt`

Copiez et collez le code suivant dans un fichier nommé `requirements.txt`.

```
boto3
pypdf
```

Dans cet exemple, le code de votre fonction ne comporte que deux dépendances qui ne font pas partie de la bibliothèque Python standard : le kit SDK pour Python (Boto3) et le package `pypdf` utilisé par la fonction pour effectuer le chiffrement du PDF.

> **Note**
>
> Une version du kit SDK pour Python (Boto3) est incluse dans l'environnement d'exécution Lambda, de sorte que votre code s'exécute sans ajouter Boto3 au package de déploiement de votre fonction. Toutefois, pour garder le contrôle total des dépendances de votre fonction et éviter d'éventuels problèmes de désalignement de version, la bonne pratique pour Python consiste à inclure toutes les dépendances de fonction dans le package de déploiement de votre fonction. Pour en savoir plus, consultez the section called "Dépendances d'exécution dans Python".

Déployer l'application

Vous pouvez créer et déployer les ressources pour cet exemple d'application manuellement ou à l'aide de AWS SAM. Dans un environnement de production, nous vous recommandons d'utiliser un outil IaC AWS SAM pour déployer rapidement et de manière répétitive des applications complètes sans serveur sans recourir à des processus manuels.

Déploiement manuel des ressources

Pour déployer votre application manuellement :

- Créez les compartiments Amazon S3 source et destination
- Créez une fonction Lambda qui chiffre un fichier PDF et enregistre la version chiffrée dans un compartiment S3
- Configurez un déclencheur Lambda qui invoque votre fonction lorsque des objets sont chargés dans votre compartiment source

Avant de commencer, assurez-vous que Python est installé sur votre machine de génération.

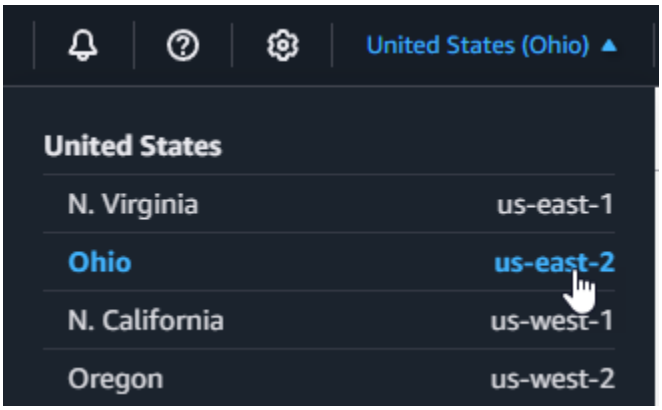
Création de deux compartiments S3

Créez deux compartiments S3. Le premier compartiment est le compartiment source dans lequel vous chargez vos fichiers PDF. Le second compartiment est utilisé par Lambda pour enregistrer les fichiers chiffrés lorsque vous invoquez votre fonction.

Console

Pour créer les compartiments S3 (console)

1. Ouvrez la page Compartiments à usage général de la console Amazon S3.
2. Sélectionnez le Région AWS plus proche de votre situation géographique. Vous pouvez modifier votre région à l'aide de la liste déroulante en haut de l'écran.



3. Choisissez Create bucket (Créer un compartiment).
4. Sous Configuration générale, procédez comme suit :
   a. Pour le type de compartiment, veillez à sélectionner Usage général.
   b. Pour le nom du compartiment, saisissez un nom unique au monde qui respecte les règles de dénomination du compartiment Amazon S3. Les noms de compartiment

peuvent contenir uniquement des lettres minuscules, des chiffres, de points (.) et des traits d'union (-).

5. Conservez les valeurs par défaut de toutes les autres options et choisissez Créer un compartiment.
6. Répétez les étapes 1 à 4 pour créer votre compartiment de destination. Pour Nom du compartiment, saisissez **`amzn-s3-demo-bucket-encrypted`**, où **`amzn-s3-demo-bucket`** est le nom du compartiment source que vous venez de créer.

AWS CLI

Avant de commencer, assurez-vous d'avoir installéAWS CLI sur la machine de génération.

Pour créer les compartiments Amazon S3 (AWS CLI)

1. Exécutez la commande CLI suivante pour créer votre compartiment source. Le nom que vous choisissez pour votre compartiment doit être unique au monde et respecter les Règles de dénomination du compartiment Amazon S3. Les noms peuvent contenir uniquement des lettres minuscules, des chiffres, de points (.) et des traits d'union (-). Pour `region` et `LocationConstraint`, choisissez la Région AWS la plus proche de votre emplacement géographique.

```
aws s3api create-bucket --bucket amzn-s3-demo-bucket --region us-east-2 \
--create-bucket-configuration LocationConstraint=us-east-2
```

   Plus loin dans le didacticiel, vous devez créer votre fonction Lambda dans le même Région AWS emplacement que votre compartiment source. Notez donc la région que vous avez choisie.
2. Exécutez la commande suivante pour créer votre compartiment de destination. Pour le nom du compartiment, vous devez utiliser **`amzn-s3-demo-bucket-encrypted`**, où **`amzn-s3-demo-bucket`** est le nom du compartiment source que vous avez créé à l'étape 1. Pour `region` et`LocationConstraint`, choisissez le même Région AWS que celui que vous avez utilisé pour créer votre bucket source.

```
aws s3api create-bucket --bucket amzn-s3-demo-bucket-encrypted --region us-
east-2 \
--create-bucket-configuration LocationConstraint=us-east-2
```

Créer un rôle d’exécution

Un rôle d'exécution est un rôle IAM qui accorde à une fonction Lambda l'autorisation d' Services AWS accès et de ressources. Pour donner à votre fonction un accès en lecture et en écriture à Amazon S3, vous attachez la politique gérée par AWS `AmazonS3FullAccess`.

Console

Créer un rôle IAM et l’attacher à la politique gérée par **`AmazonS3FullAccess`** (console)

1. Ouvrez la page Roles (Rôles) dans la console IAM.
2. Choisissez Créer un rôle.
3. Pour Type d’entité approuvée, sélectionnez Service AWS , et pour Cas d’utilisation, sélectionnez Lambda.
4. Choisissez Suivant.
5. Ajoutez la politique gérée `AmazonS3FullAccess` en procédant comme suit :
   a. Dans Politiques d’autorisations, saisissez **`AmazonS3FullAccess`** dans la barre de recherche.
   b. Activez la case à cocher en regard de la stratégie.
   c. Choisissez Suivant.
6. Dans Détails du rôle, saisissez **`LambdaS3Role`** pour Nom du rôle.
7. Choisissez Créer un rôle.

AWS CLI

Pour créer un rôle d'exécution et associer la politique **`AmazonS3FullAccess`**gérée (AWS CLI)

1. Enregistrez le JSON suivant dans un fichier nommé `trust-policy.json`. Cette politique de confiance permet à Lambda d'utiliser les autorisations du rôle en autorisant le principal `lambda.amazonaws.com` du service à appeler l'action AWS Security Token Service (AWS STS)`AssumeRole`.

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
```

```
      "Effect": "Allow",
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

2. À partir du répertoire dans lequel vous avez enregistré le document de politique d'approbation JSON, exécutez la commande CLI suivante pour créer le rôle d'exécution.

```
aws iam create-role --role-name LambdaS3Role --assume-role-policy-document
 file://trust-policy.json
```

3. Pour associer la politique gérée `AmazonS3FullAccess`, exécutez la commande de la CLI suivante.

```
aws iam attach-role-policy --role-name LambdaS3Role --policy-arn
 arn:aws:iam::aws:policy/AmazonS3FullAccess
```

Créer le package de déploiement de la fonction

Pour créer votre fonction, vous créez un package de déploiement contenant le code de votre fonction et ses dépendances. Pour cette application, votre code de fonction utilise une bibliothèque distincte pour le chiffrement du PDF.

Pour créer le package de déploiement

1. Accédez au répertoire du projet contenant les `requirements.txt` fichiers `lambda_function.py` et que vous avez créés ou téléchargés GitHub précédemment et créez un nouveau répertoire nommé`package`.
2. Installez les dépendances spécifiées dans le fichier `requirements.txt` de votre répertoire `package` en exécutant la commande suivante.

```
pip install -r requirements.txt --target ./package/
```

3. Créez un fichier .zip contenant le code de votre application et ses dépendances. Sous Linux ou macOS, exécutez les commandes suivantes depuis votre interface de ligne de commande.

```
cd package
zip -r ../lambda_function.zip .
cd ..
zip lambda_function.zip lambda_function.py
```

Sous Windows, utilisez l'outil zip de votre choix pour créer le fichier `lambda_function.zip`. Assurez-vous que votre fichier `lambda_function.py` et les dossiers contenant vos dépendances sont installés à la racine du fichier .zip.

Vous pouvez également créer votre package de déploiement à l'aide d'un environnement virtuel Python. Consultez Utilisation d'archives de fichiers .zip pour les fonctions événementielles Lambda en Python

Créer la fonction Lambda

Vous utilisez maintenant le package de déploiement que vous avez créé à l'étape précédente pour déployer votre fonction Lambda.

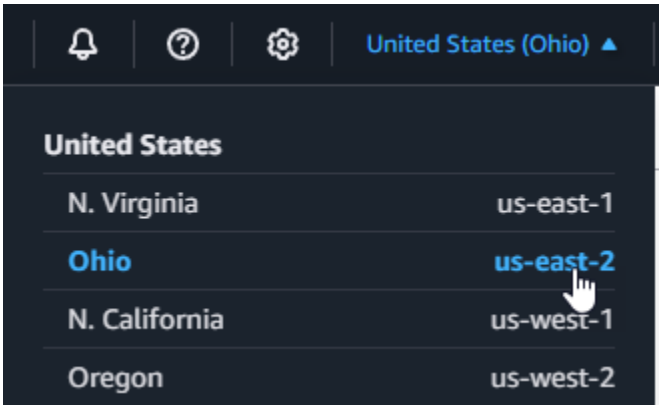
Console

Pour créer une fonction (console)

Pour créer votre fonction Lambda à l'aide de la console, vous devez d'abord créer une fonction de base contenant du code « Hello world ». Vous remplacez ensuite ce code par votre propre code de fonction en chargeant le fichier .zip que vous avez créé à l'étape précédente.

Pour garantir que votre fonction n'expire pas lors du chiffrement de fichiers PDF volumineux, configurez les paramètres de mémoire et de délai d'expiration de la fonction. Définissez également le format de journal de la fonction sur JSON. La configuration de journaux au format JSON est nécessaire lors de l'utilisation du script de test fourni afin que celui-ci puisse lire l'état d'invocation de la fonction dans CloudWatch Logs pour confirmer la réussite de l'appel.

1. Ouvrez la page Event Functions de la console Lambda.
2. Assurez-vous de travailler dans le même environnement que celui dans Région AWS lequel vous avez créé votre compartiment S3. Vous pouvez modifier votre région à l'aide de la liste déroulante en haut de l'écran.



3. Choisissez Create Event Function.
4. Choisissez Créer à partir de zéro.
5. Sous Informations de base, procédez comme suit :

   a. Sous Nom de la fonction, saisissez **`EncryptPDF`**.

   b. Pour Environnement d'exécution, choisissez Python 3.12.

   c. Pour Architecture, choisissez x86_64.
6. Associez le rôle d'exécution que vous avez créé à l'étape précédente en procédant comme suit :

   a. Développez la section Changer le rôle d'exécution par défaut.

   b. Sélectionnez Utiliser un rôle existant.

   c. Sous Rôle existant, sélectionnez votre rôle (`LambdaS3Role`).
7. Choisissez Create Event Function.

Pour charger le code de fonction (console)

1. Dans le volet Source du code, choisissez Charger à partir de.
2. Choisissez Fichier .zip.
3. Choisissez Charger.
4. Dans le sélecteur de fichiers, sélectionnez votre fichier .zip et choisissez Ouvrir.
5. Cliquez sur Enregistrer.

Pour configurer la mémoire et le délai d'expiration d'une fonction (console)

1. Sélectionnez l'onglet Configuration correspondant à votre fonction.

2. Dans le volet de Configuration générale, choisissez Modifier.
3. Réglez Mémoire sur 256 Mo et Délai d'expiration sur 15 secondes.
4. Cliquez sur Enregistrer.

Pour configurer le format de journal (console)

1. Sélectionnez l'onglet Configuration correspondant à votre fonction.
2. Sélectionnez Outils de surveillance et d'exploitation.
3. Dans le volet de configuration de la journalisation, choisissez Modifier.
4. Pour Configuration de journalisation, sélectionnez JSON.
5. Cliquez sur Enregistrer.

AWS CLI

Pour créer la fonction (AWS CLI)

- Exécutez la commande suivante depuis le répertoire contenant votre fichier `lambda_function.zip`. Pour le paramètre `region`, remplacez `us-east-2` par la région dans laquelle vous avez créé vos compartiments S3.

```
aws lambda create-function --function-name EncryptPDF \
--zip-file fileb://lambda_function.zip --handler lambda_function.lambda_handler
 \
--runtime python3.12 --timeout 15 --memory-size 256 \
--role arn:aws:iam::123456789012:role/LambdaS3Role --region us-east-2 \
--logging-config LogFormat=JSON
```

Configuration d'un déclencheur Amazon S3 pour invoquer la fonction

Pour que votre fonction Lambda s'exécute lorsque vous chargez un fichier dans votre compartiment source, vous devez configurer un déclencheur pour votre fonction. Vous pouvez configurer le déclencheur Amazon S3 à l'aide de la console ou de la AWS CLI.

> **Important**
>
> Cette procédure configure le compartiment S3 pour qu'il invoque votre fonction chaque fois qu'un objet est créé dans le compartiment. Veillez à configurer cela uniquement pour le

compartiment source. Si votre fonction Lambda crée des objets dans le même compartiment que celui qui l'invoque, votre fonction peut être invoquée en continu dans une boucle. Cela peut entraîner la facturation de frais imprévus à votre Compte AWS charge.

Console

Pour configurer le déclencheur Amazon S3 (console)

1. Ouvrez la page Event Functions de la console Lambda et choisissez votre fonction ()`EncryptPDF`.
2. Choisissez Add trigger (Ajouter déclencheur).
3. Sélectionnez S3.
4. Sous Compartiment, sélectionnez votre compartiment source.
5. Sous Types d'événements, sélectionnez Tous les événements de création d'objets.
6. Sous Invocation récursive, cochez la case pour confirmer qu'il n'est pas recommandé d'utiliser le même compartiment S3 pour les entrées et les sorties. Vous pouvez en savoir plus sur les modèles d'invocation récursive dans Lambda en lisant la rubrique Modèles récursifs qui provoquent des fonctions Lambda incontrôlables dans Serverless Land.
7. Choisissez Ajouter.

   Lorsque vous créez un déclencheur à l'aide de la console Lambda, ce dernier crée automatiquement une politique basée sur une ressource pour donner au service que vous sélectionnez l'autorisation d'invoquer votre fonction.

AWS CLI

Pour configurer le déclencheur Amazon S3 (AWS CLI)

1. Ajoutez une politique basée sur les ressources à votre fonction qui permet à votre compartiment source Amazon S3 d'invoquer votre fonction lorsque vous ajoutez un fichier. Une déclaration de politique basée sur les ressources donne à d'autres personnes Services AWS l'autorisation d'invoquer votre fonction. Pour autoriser Amazon S3 à invoquer votre fonction, exécutez la commande CLI suivante. Assurez-vous de remplacer le `source-account` paramètre par votre propre Compte AWS identifiant et d'utiliser votre propre nom de compartiment source.

```
aws lambda add-permission --function-name EncryptPDF \
--principal s3.amazonaws.com --statement-id s3invoke --action
 "lambda:InvokeFunction" \
--source-arn arn:aws:s3:::amzn-s3-demo-bucket \
--source-account 123456789012
```

La politique que vous définissez à l'aide de cette commande permet à Amazon S3 d'invoquer votre fonction uniquement lorsqu'une action a lieu sur votre compartiment source.

> **Note**
>
> Bien que les noms des compartiments S3 soient globalement uniques, il est préférable de spécifier que le compartiment doit appartenir à votre compte lorsque vous utilisez des politiques basées sur les ressources. En effet, si vous supprimez un bucket, il est possible qu'un autre Compte AWS en crée un avec le même Amazon Resource Name (ARN).

2. Enregistrez le JSON suivant dans un fichier nommé `notification.json`. Lorsqu'il est appliqué à votre compartiment source, ce JSON configure le compartiment pour qu'il envoie une notification à votre fonction Lambda chaque fois qu'un nouvel objet est ajouté. Remplacez le Compte AWS numéro et, Région AWS dans la fonction Lambda, l'ARN par votre propre numéro de compte et votre propre région.

```
{
"LambdaFunctionConfigurations": [
    {
      "Id": "EncryptPDFEventConfiguration",
      "LambdaFunctionArn": "arn:aws:lambda:us-
east-2:123456789012:function:EncryptPDF",
      "Events": [ "s3:ObjectCreated:Put" ]
    }
  ]
}
```

3. Exécutez la commande CLI suivante pour appliquer les paramètres de notification du fichier JSON que vous avez créé à votre compartiment source. Remplacez `amzn-s3-demo-bucket` par le nom de votre propre compartiment source.

```
aws s3api put-bucket-notification-configuration --bucket amzn-s3-demo-bucket \
```

```
--notification-configuration file://notification.json
```

Pour en savoir plus sur la commande `put-bucket-notification-configuration` et l'option `notification-configuration`, consultez la section put-bucket-notification-configuration dans la référence des commandes de la CLI AWS .

Déployez les ressources à l'aide de AWS SAM

Avant de commencer, assurez-vous que Docker et la dernière version de AWS SAMCLI sont installés sur votre machine de génération.

1. Dans le répertoire de votre projet, copiez et collez le code suivant dans un fichier nommé `template.yaml`. Remplacez les espaces réservés des noms des compartiments :

   - Pour le compartiment source, remplacez `amzn-s3-demo-bucket` par un nom conforme aux règles de dénomination des compartiments S3.
   - Pour le compartiment de destination, remplacez `amzn-s3-demo-bucket-encrypted` par `<source-bucket-name>-encrypted`, où `<source-bucket>` est le nom que vous avez choisi pour votre compartiment source.

```
AWSTemplateFormatVersion: '2010-09-09'
Transform: AWS::Serverless-2016-10-31

Resources:
  EncryptPDFFunction:
    Type: AWS::Serverless::Function
    Properties:
      FunctionName: EncryptPDF
      Architectures: [x86_64]
      CodeUri: ./
      Handler: lambda_function.lambda_handler
      Runtime: python3.12
      Timeout: 15
      MemorySize: 256
      LoggingConfig:
        LogFormat: JSON
      Policies:
        - AmazonS3FullAccess
      Events:
        S3Event:
```

```
          Type: S3
          Properties:
            Bucket: !Ref PDFSourceBucket
            Events: s3:ObjectCreated:*

  PDFSourceBucket:
    Type: AWS::S3::Bucket
    Properties:
      BucketName: amzn-s3-demo-bucket

  EncryptedPDFBucket:
    Type: AWS::S3::Bucket
    Properties:
      BucketName: amzn-s3-demo-bucket-encrypted
```

Le AWS SAM modèle définit les ressources que vous créez pour votre application. Dans cet exemple, le modèle définit une fonction Lambda utilisant le type `AWS::Serverless::Function` et deux compartiments S3 utilisant le type `AWS::S3::Bucket`. Les noms de compartiments spécifiés dans le modèle sont des espaces réservés. Avant de déployer l'application à l'aide de AWS SAM, vous devez modifier le modèle pour renommer les compartiments avec des noms uniques au niveau mondial conformes aux règles de dénomination des compartiments S3. Cette étape est expliquée plus en détail dans the section called “Déployez les ressources à l'aide de AWS SAM”.

La définition de la ressource de fonction Lambda configure un déclencheur pour la fonction à l’aide de la propriété d’événement `S3Event`. Ce déclencheur entraîne l’invocation de votre fonction chaque fois qu’un objet est créé dans votre compartiment source.

La définition de la fonction spécifie également une politique Gestion des identités et des accès AWS (IAM) à associer au rôle d'exécution de la fonction. La politique gérée par AWS `AmazonS3FullAccess` donne à votre fonction les autorisations dont elle a besoin pour lire et écrire des objets sur Amazon S3.

2. Exécutez la commande suivante dans le répertoire où vous avez enregistré les fichiers `template.yaml`, `lambda_function.py` et `requirements.txt`.

```
sam build --use-container
```

Cette commande rassemble les artefacts de compilation pour votre application et les place dans le format et l’emplacement appropriés pour les déployer. La spécification de l'`--use-`

`container`option crée votre fonction dans un conteneur Lambda-like Docker. Nous l'utilisons ici, vous n'avez donc pas besoin d'installer Python 3.12 sur votre machine locale pour que la compilation fonctionne.

Pendant le processus de génération, AWS SAM recherche le code de la fonction Lambda à l'emplacement que vous avez spécifié avec la `CodeUri` propriété dans le modèle. Dans ce cas, nous avons spécifié le répertoire actuel comme emplacement (`./`).

Si un `requirements.txt` fichier est présent, AWS SAM utilisez-le pour rassembler les dépendances spécifiées. Par défaut, AWS SAM crée un package de déploiement .zip avec le code de votre fonction et ses dépendances. Vous pouvez également choisir de déployer votre fonction sous forme d'image de conteneur à l'aide de la PackageTypepropriété.

3. Pour déployer votre application et créer les ressources Lambda et Amazon S3 spécifiées dans votre AWS SAM modèle, exécutez la commande suivante.

```
sam deploy --guided
```

L'utilisation du `--guided` drapeau signifie que des instructions vous AWS SAM seront affichées pour vous guider tout au long du processus de déploiement. Pour ce déploiement, acceptez les options par défaut en appuyant sur Entrée.

Au cours du processus de déploiement, AWS SAM crée les ressources suivantes dans votre Compte AWS :

- Une CloudFormation pile nommée `sam-app`
- Une fonction Lambda nommée `EncryptPDF`
- Deux compartiments S3 portant les noms que vous avez choisis lorsque vous avez modifié le `template.yaml` AWS SAM fichier modèle
- Un rôle d'exécution IAM pour votre fonction avec le format de nom `sam-app-EncryptPDFFunctionRole-`*`2qGaapHFWOQ8`*

Lorsque vous avez AWS SAM terminé de créer vos ressources, le message suivant devrait s'afficher :

```
Successfully created/updated stack - sam-app in us-east-2
```

Tester l'application

Pour tester votre application, chargez un fichier PDF dans votre compartiment source et vous confirmez que Lambda crée une version chiffrée du fichier dans votre compartiment de destination. Dans cet exemple, vous pouvez le tester manuellement à l'aide de la AWS CLI console ou du script de test fourni.

Pour les applications de production, vous pouvez utiliser des méthodes et techniques de test traditionnelles, telles que les tests unitaires, pour confirmer le bon fonctionnement de votre code de fonction Lambda. Les pratiques exemplaires consistent également à effectuer des tests comme ceux du script de test fourni, qui réalisent des tests d'intégration avec des ressources réelles, basées sur le cloud. Les tests d'intégration dans le cloud confirment que votre infrastructure a été correctement déployée et que les événements circulent entre les différents services comme prévu. Pour en savoir plus, consultez the section called "Tests".

Test manuel de l'application

Vous pouvez tester votre fonction manuellement en ajoutant un fichier PDF à votre compartiment source Amazon S3. Lorsque vous ajoutez votre fichier au compartiment source, votre fonction Lambda doit être automatiquement invoquée et doit stocker une version chiffrée du fichier dans votre compartiment cible.

Console

Pour tester votre application en chargeant un fichier (console)

1. Pour charger un fichier PDF dans votre compartiment S3, procédez comme suit :
   a. Ouvrez la page Compartiments de la console Amazon S3 et choisissez votre compartiment source.
   b. Choisissez Charger.
   c. Choisissez Ajouter des fichiers et utilisez le sélecteur de fichiers pour sélectionner le fichier PDF que vous souhaitez charger.
   d. Choisissez Ouvrir, puis Charger.
2. Vérifiez que Lambda a enregistré une version chiffrée de votre fichier PDF dans votre compartiment cible en procédant comme suit :
   a. Retournez à la page Compartiments de la console Amazon S3 et choisissez votre compartiment de destination.

b. Dans le volet Objets, vous devriez maintenant voir un fichier au format de nom `filename_encrypted.pdf` (où `filename.pdf` était le nom du fichier que vous avez chargé dans votre compartiment source). Pour télécharger votre PDF chiffré, sélectionnez le fichier, puis choisissez Télécharger.

c. Vérifiez que vous pouvez ouvrir le fichier téléchargé avec le mot de passe avec lequel votre fonction Lambda l'a protégé (`my-secret-password`).

AWS CLI

Pour tester votre application en chargeant un fichier (AWS CLI)

1. À partir du répertoire contenant le fichier PDF que vous souhaitez charger, exécutez la commande de la CLI suivante. Remplacez le paramètre `--bucket` par le nom de votre compartiment source. Pour les paramètres `--key` et `--body`, utilisez le nom de fichier de votre fichier de test.

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key test.pdf --body ./
test.pdf
```

2. Vérifiez que votre fonction a créé une version chiffrée de votre fichier et l'a enregistrée dans votre compartiment S3 cible. Exécutez la commande CLI suivante, en remplaçant `amzn-s3-demo-bucket-encrypted` par le nom de votre compartiment de destination.

```
aws s3api list-objects-v2 --bucket amzn-s3-demo-bucket-encrypted
```

Si votre fonction s'exécute correctement, vous obtiendrez un résultat similaire à ce qui suit. Votre compartiment cible doit contenir un fichier au format de nom *<your_test_file>*`_encrypted.pdf`, où `<your_test_file>` est le nom du fichier que vous avez chargé.

```
{
    "Contents": [
        {
            "Key": "test_encrypted.pdf",
            "LastModified": "2023-06-07T00:15:50+00:00",
            "ETag": "\"7781a43e765a8301713f533d70968a1e\"",
            "Size": 2763,
            "StorageClass": "STANDARD"
        }
```

```
    ]
}
```

3. Pour télécharger le fichier que Lambda a enregistré dans votre compartiment de destination, exécutez la commande de la CLI suivante. Remplacez le paramètre `--bucket` par le nom de votre compartiment de destination. Pour le paramètre `--key`, utilisez le nom de fichier *<your_test_file>*`_encrypted.pdf`, où <your_test_file> est le nom du fichier de test que vous avez chargé.

```
aws s3api get-object --bucket amzn-s3-demo-bucket-encrypted --
key test_encrypted.pdf my_encrypted_file.pdf
```

   Cette commande télécharge le fichier dans votre répertoire actuel et l'enregistre sous `my_encrypted_file.pdf`.
4. Vérifiez que vous pouvez ouvrir le fichier téléchargé avec le mot de passe avec lequel votre fonction Lambda l'a protégé (`my-secret-password`).

Test de l'application avec le script automatique

Créez les fichiers suivants dans le répertoire de votre projet :

- `test_pdf_encrypt.py` : un script de test que vous pouvez utiliser pour tester automatiquement votre application
- `pytest.ini` : un fichier de configuration pour le script de test

Développez les sections suivantes pour afficher le code et pour en savoir plus sur le rôle de chaque fichier.

Script de test automatisé

Copiez et collez le code suivant dans un fichier nommé `test_pdf_encrypt.py`. Veillez à remplacer les espaces réservés de nom de compartiment :

- Dans la fonction `test_source_bucket_available`, remplacez `amzn-s3-demo-bucket` par le nom de votre compartiment source.
- Dans la fonction `test_encrypted_file_in_bucket`, remplacez `amzn-s3-demo-bucket-encrypted` par *source-bucket*`-encrypted`, où source-bucket> est le nom de votre compartiment source.

- Dans la fonction `cleanup`, remplacez `amzn-s3-demo-bucket` par le nom de votre compartiment source et remplacez `amzn-s3-demo-bucket-encrypted` par le nom de votre compartiment source.

```
import boto3
import json
import pytest
import time
import os

@pytest.fixture
def lambda_client():
    return boto3.client('lambda')

@pytest.fixture
def s3_client():
    return boto3.client('s3')

@pytest.fixture
def logs_client():
    return boto3.client('logs')

@pytest.fixture(scope='session')
def cleanup():
    # Create a new S3 client for cleanup
    s3_client = boto3.client('s3')

    yield
    # Cleanup code will be executed after all tests have finished

    # Delete test.pdf from the source bucket
    source_bucket = 'amzn-s3-demo-bucket'
    source_file_key = 'test.pdf'
    s3_client.delete_object(Bucket=source_bucket, Key=source_file_key)
    print(f"\nDeleted {source_file_key} from {source_bucket}")

    # Delete test_encrypted.pdf from the destination bucket
    destination_bucket = 'amzn-s3-demo-bucket-encrypted'
    destination_file_key = 'test_encrypted.pdf'
    s3_client.delete_object(Bucket=destination_bucket, Key=destination_file_key)
    print(f"Deleted {destination_file_key} from {destination_bucket}")
```

```
@pytest.mark.order(1)
def test_source_bucket_available(s3_client):
    s3_bucket_name = 'amzn-s3-demo-bucket'
    file_name = 'test.pdf'
    file_path = os.path.join(os.path.dirname(__file__), file_name)

    file_uploaded = False
    try:
        s3_client.upload_file(file_path, s3_bucket_name, file_name)
        file_uploaded = True
    except:
        print("Error: couldn't upload file")

    assert file_uploaded, "Could not upload file to S3 bucket"



@pytest.mark.order(2)
def test_lambda_invoked(logs_client):

    # Wait for a few seconds to make sure the logs are available
    time.sleep(5)

    # Get the latest log stream for the specified log group
    log_streams = logs_client.describe_log_streams(
        logGroupName='/aws/lambda/EncryptPDF',
        orderBy='LastEventTime',
        descending=True,
        limit=1
    )

    latest_log_stream_name = log_streams['logStreams'][0]['logStreamName']

    # Retrieve the log events from the latest log stream
    log_events = logs_client.get_log_events(
        logGroupName='/aws/lambda/EncryptPDF',
        logStreamName=latest_log_stream_name
    )

    success_found = False
    for event in log_events['events']:
        message = json.loads(event['message'])
        status = message.get('record', {}).get('status')
```

```
        if status == 'success':
            success_found = True
            break

    assert success_found, "Lambda function execution did not report 'success' status in
 logs."

@pytest.mark.order(3)
def test_encrypted_file_in_bucket(s3_client):
    # Specify the destination S3 bucket and the expected converted file key
    destination_bucket = 'amzn-s3-demo-bucket-encrypted'
    converted_file_key = 'test_encrypted.pdf'

    try:
        # Attempt to retrieve the metadata of the converted file from the destination
 S3 bucket
        s3_client.head_object(Bucket=destination_bucket, Key=converted_file_key)
    except s3_client.exceptions.ClientError as e:
        # If the file is not found, the test will fail
        pytest.fail(f"Converted file '{converted_file_key}' not found in the
 destination bucket: {str(e)}")

def test_cleanup(cleanup):
    # This test uses the cleanup fixture and will be executed last
    pass
```

Le script de test automatique exécute trois fonctions de test pour confirmer le bon fonctionnement de votre application :

- Le test `test_source_bucket_available` confirme que votre compartiment source a été créé avec succès en y téléchargeant un fichier PDF de test.
- Le test `test_lambda_invoked` interroge le dernier flux du journal CloudWatch Logs de votre fonction afin de confirmer que lorsque vous avez chargé le fichier de test, votre fonction Lambda s'est exécutée et a signalé un succès.
- Le test `test_encrypted_file_in_bucket` confirme que votre compartiment de destination contient le fichier chiffré `test_encrypted.pdf`.

Une fois tous ces tests exécutés, le script exécute une étape de nettoyage supplémentaire pour supprimer les fichiers `test.pdf` et `test_encrypted.pdf` de vos compartiments source et de destination.

Comme pour le AWS SAM modèle, les noms de compartiments spécifiés dans ce fichier sont des espaces réservés. Avant d'exécuter le test, vous devez modifier ce fichier avec les noms de compartiment réels de votre application. Cette étape est expliquée plus en détail dans the section called "Test de l'application avec le script automatique".

Fichier de configuration du script de test

Copiez et collez le code suivant dans un fichier nommé `pytest.ini`.

```
[pytest]
markers =
    order: specify test execution order
```

Cela est nécessaire pour spécifier l'ordre dans lequel les tests du script `test_pdf_encrypt.py` s'exécutent.

Pour exécuter l'exemple, procédez comme suit :

1. Assurez-vous que le module `pytest` est installé dans votre environnement local. Vous pouvez installer `pytest` en exécutant les commandes suivantes :

   ```
   pip install pytest
   ```

2. Enregistrez un fichier PDF nommé `test.pdf` dans le répertoire contenant les fichiers `test_pdf_encrypt.py` et `pytest.ini`.
3. Ouvrez un terminal ou un exécuteur shell et exécutez la commande suivante depuis le répertoire contenant les fichiers de test.

   ```
   pytest -s -v
   ```

   Lorsque le test est terminé, vous devriez obtenir un résultat semblable à celui qui suit :

   ```
   ============================================================= test session starts
    ============================================================
   platform linux -- Python 3.12.2, pytest-7.2.2, pluggy-1.0.0 -- /usr/bin/python3
   cachedir: .pytest_cache
   hypothesis profile 'default' -> database=DirectoryBasedExampleDatabase('/home/
   pdf_encrypt_app/.hypothesis/examples')
   Test order randomisation NOT enabled. Enable with --random-order or --random-order-
   bucket=<bucket_type>
   ```

```
rootdir: /home/pdf_encrypt_app, configfile: pytest.ini
plugins: anyio-3.7.1, hypothesis-6.70.0, localserver-0.7.1, random-order-1.1.0
collected 4 items

test_pdf_encrypt.py::test_source_bucket_available PASSED
test_pdf_encrypt.py::test_lambda_invoked PASSED
test_pdf_encrypt.py::test_encrypted_file_in_bucket PASSED
test_pdf_encrypt.py::test_cleanup PASSED
Deleted test.pdf from amzn-s3-demo-bucket
Deleted test_encrypted.pdf from amzn-s3-demo-bucket-encrypted


============================================================== 4 passed in 7.32s
 ===============================================================
```

Étapes suivantes

Maintenant que vous avez créé cet exemple d'application, vous pouvez utiliser le code fourni comme base pour créer d'autres types d'applications de traitement de fichiers. Modifiez le code du fichier `lambda_function.py` pour mettre en œuvre la logique de traitement de fichiers adaptée à votre cas d'utilisation.

De nombreux cas d'utilisation typiques du traitement de fichiers impliquent le traitement d'image. Lorsque vous utilisez Python, les bibliothèques de traitement d'image les plus populaires telles que pillow contiennent généralement des composants C ou C++. Pour garantir que le package de déploiement de votre fonction est compatible avec l'environnement d'exécution Lambda, il est important d'utiliser le bon binaire de distribution source.

Lorsque vous déployez vos ressources avec AWS SAM, vous devez prendre des mesures supplémentaires pour inclure la distribution source appropriée dans votre package de déploiement. Étant donné que les dépendances AWS SAM ne seront pas installées pour une plate-forme différente de celle de votre machine de génération, la spécification de la distribution source (`.whl`fichier) correcte dans votre `requirements.txt` fichier ne fonctionnera pas si votre machine de génération utilise un système d'exploitation ou une architecture différent de l'environnement d'exécution Lambda. Au lieu de cela, vous devriez procéder à l'une des opérations suivantes :

- Utilisez l'option `--use-container` lors de l'exécution de `sam build`. Lorsque vous spécifiez cette option, AWS SAM télécharge une image de base de conteneur compatible avec l'environnement d'exécution Lambda et crée le package de déploiement de votre fonction dans

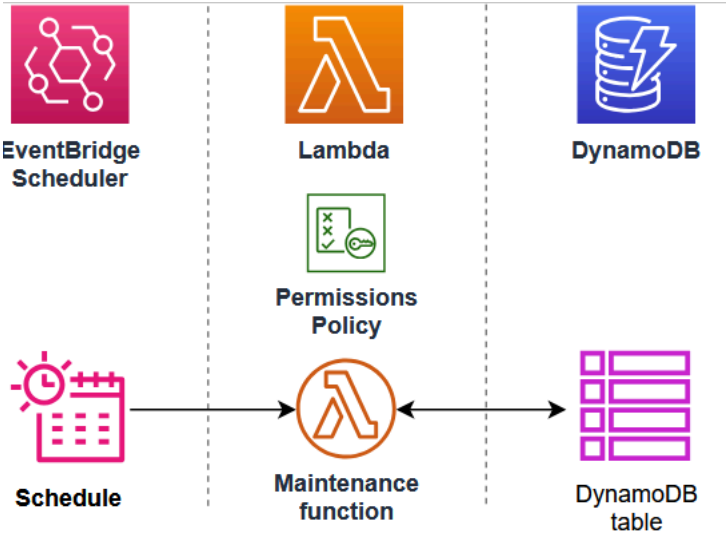
un conteneur Docker à l'aide de cette image. Pour en savoir plus, consultez Building a Lambda function inside of a provided container.

- Créez vous-même le package de déploiement .zip de votre fonction en utilisant le binaire de distribution source approprié et enregistrez le fichier .zip dans le répertoire que vous spécifiez `CodeUri` dans le AWS SAM modèle. Pour en savoir plus sur la création de packages de déploiement .zip pour Python à l'aide de distributions binaires, consultez the section called "Création d'un package de déploiement .zip avec dépendances" et the section called "Création de packages de déploiement .zip avec des bibliothèques natives".

Création d'une application de maintenance planifiée de la base de données

Vous pouvez l'utiliser AWS Lambda pour remplacer les processus planifiés tels que les sauvegardes automatisées du système, les conversions de fichiers et les tâches de maintenance. Dans cet exemple, vous créez une application sans serveur qui effectue une maintenance planifiée régulière sur une table DynamoDB en supprimant les anciennes entrées. L'application utilise EventBridge Scheduler pour appeler une fonction Lambda selon un calendrier cron. Lorsqu'elle est invoquée, la fonction rechercher dans la table pour les éléments datant de plus d'un an et les supprime. La fonction enregistre chaque élément supprimé dans CloudWatch Logs.

Pour implémenter cet exemple, créez d'abord une table DynamoDB et remplissez-la avec des données de test que votre fonction doit interroger. Créez ensuite une fonction Lambda Python avec un déclencheur EventBridge Scheduler et un rôle d'exécution IAM qui autorise la fonction à lire et à supprimer des éléments de votre table.



> **Tip**
>
> Si vous utilisez Lambda pour la première fois, nous vous recommandons de suivre le didacticiel the section called “Création de votre première fonction” avant de créer cet exemple d'application.

Vous pouvez déployer votre application manuellement en créant et en configurant des ressources à l'aide du Console de gestion AWS. Vous pouvez également déployer l'application en utilisant le AWS Serverless Application Model (AWS SAM). AWS SAM est un outil d'infrastructure en tant que code (IaC). Avec IaC, vous ne créez pas de ressources manuellement, mais vous les définissez dans le code, puis vous les déployez automatiquement.

Si vous souhaitez en savoir plus sur l’utilisation de Lambda avec l’IaC avant de déployer cet exemple d’application, consultez the section called “Infrastructure en tant que code (IaC)”.

Conditions préalables

Avant de créer l’exemple d’application, assurez-vous que les outils et programmes de ligne de commande requis sont installés.

- Python

  Pour remplir la table DynamoDB que vous créez pour tester votre application, cet exemple utilise un script Python et un fichier CSV pour écrire des données dans la table. Assurez-vous que Python 3.8 ou version ultérieure est installé sur votre machine.
- AWS SAM INTERFACE DE LIGNE DE COMMANDE (CLI)

  Si vous souhaitez créer la table DynamoDB et déployer l'exemple d'application à l' AWS SAM aide, vous devez installer la CLI. AWS SAM Suivez les instructions d’installation dans le Guise de l’utilisateur AWS SAM .
- AWS CLI

  Pour utiliser le script Python fourni pour remplir votre table de test, vous devez avoir installé et configuré l’ AWS CLI. Cela est dû au fait que le script utilise le AWS SDK pour Python (Boto3), qui doit accéder à vos informations d'identification Gestion des identités et des accès AWS (IAM). Vous devez également l' AWS CLI installer pour déployer des ressources à l'aide de AWS SAM. Installez la CLI en suivant les instructions d’installation du Guide de l’utilisateur AWS Command Line Interface .

- Docker

  Pour déployer l'application à l'aide de Docker AWS SAM, vous devez également être installé sur votre machine de compilation. Suivez les instructions dans Install Docker Engine sur le site Web de documentation de Docker.

Téléchargement des exemples de fichiers d’application

Pour créer la base de données d’exemple et l’application de maintenance planifiée, vous devez créer les fichiers suivants dans le répertoire de votre projet :

Exemples de fichiers de base de données

- `template.yaml`- un AWS SAM modèle que vous pouvez utiliser pour créer la table DynamoDB
- `sample_data.csv` : un fichier CSV contenant des exemples de données à charger dans votre tableau
- `load_sample_data.py` : un script Python qui écrit les données du fichier CSV dans le tableau

Scheduled-maintenance fichiers d'application

- `lambda_function.py` : le code de fonction Python de la fonction Lambda qui effectue la maintenance de la base de données
- `requirements.txt` : un fichier manifeste définissant les dépendances requises par le code de votre fonction Python
- `template.yaml`- un AWS SAM modèle que vous pouvez utiliser pour déployer l'application

Fichier de test

- `test_app.py` : un script Python qui scanne la table et confirme le bon fonctionnement de votre fonction en affichant tous les enregistrements datant de plus d’un an

Développez les sections suivantes pour afficher le code et pour en savoir plus sur le rôle de chaque fichier dans la création et le test de votre application. Pour créer les fichiers sur votre ordinateur local, copiez et collez le code ci-dessous.

AWS SAM modèle (exemple de table DynamoDB)

Copiez et collez le code suivant dans un fichier nommé `template.yaml`.

```
AWSTemplateFormatVersion: '2010-09-09'
Transform: AWS::Serverless-2016-10-31
Description: SAM Template for DynamoDB Table with Order_number as Partition Key and
 Date as Sort Key

Resources:
  MyDynamoDBTable:
    Type: AWS::DynamoDB::Table
    DeletionPolicy: Retain
    UpdateReplacePolicy: Retain
    Properties:
      TableName: MyOrderTable
      BillingMode: PAY_PER_REQUEST
      AttributeDefinitions:
        - AttributeName: Order_number
          AttributeType: S
        - AttributeName: Date
          AttributeType: S
      KeySchema:
        - AttributeName: Order_number
          KeyType: HASH
        - AttributeName: Date
          KeyType: RANGE
      SSESpecification:
        SSEEnabled: true
      GlobalSecondaryIndexes:
        - IndexName: Date-index
          KeySchema:
            - AttributeName: Date
              KeyType: HASH
          Projection:
            ProjectionType: ALL
      PointInTimeRecoverySpecification:
        PointInTimeRecoveryEnabled: true

Outputs:
  TableName:
    Description: DynamoDB Table Name
    Value: !Ref MyDynamoDBTable
  TableArn:
```

```
    Description: DynamoDB Table ARN
    Value: !GetAtt MyDynamoDBTable.Arn
```

> **Note**
>
> AWS SAM les modèles utilisent une convention de dénomination standard `detemplate.yaml`. Dans cet exemple, vous disposez de deux fichiers modèles : l'un pour créer la base de données d'exemple et l'autre pour créer l'application elle-même. Enregistrez-les dans des sous-répertoires distincts dans votre dossier de projet.

Ce AWS SAM modèle définit la ressource de table DynamoDB que vous créez pour tester votre application. La table utilise une clé primaire `Order_number` avec une clé de tri `Date`. Pour que votre fonction Lambda puisse rechercher des éléments directement par date, nous définissons également un index secondaire global nommé `Date-index`.

Pour en savoir plus sur la création et la configuration d'une table DynamoDB à l'aide de cette ressource `AWS::DynamoDB::Table`, consultez AWS::DynamoDB::Table dans le Guide de l'utilisateur AWS CloudFormation .

Exemple de fichier de données de base de données

Copiez et collez le code suivant dans un fichier nommé `sample_data.csv`.

```
Date,Order_number,CustomerName,ProductID,Quantity,TotalAmount
2023-09-01,ORD001,Alejandro Rosalez,PROD123,2,199.98
2023-09-01,ORD002,Akua Mansa,PROD456,1,49.99
2023-09-02,ORD003,Ana Carolina Silva,PROD789,3,149.97
2023-09-03,ORD004,Arnav Desai,PROD123,1,99.99
2023-10-01,ORD005,Carlos Salazar,PROD456,2,99.98
2023-10-02,ORD006,Diego Ramirez,PROD789,1,49.99
2023-10-03,ORD007,Efua Owusu,PROD123,4,399.96
2023-10-04,ORD008,John Stiles,PROD456,2,99.98
2023-10-05,ORD009,Jorge Souza,PROD789,3,149.97
2023-10-06,ORD010,Kwaku Mensah,PROD123,1,99.99
2023-11-01,ORD011,Li Juan,PROD456,5,249.95
2023-11-02,ORD012,Marcia Oliveria,PROD789,2,99.98
2023-11-03,ORD013,Maria Garcia,PROD123,3,299.97
2023-11-04,ORD014,Martha Rivera,PROD456,1,49.99
2023-11-05,ORD015,Mary Major,PROD789,4,199.96
2023-12-01,ORD016,Mateo Jackson,PROD123,2,199.99
```

```
2023-12-02,ORD017,Nikki Wolf,PROD456,3,149.97
2023-12-03,ORD018,Pat Candella,PROD789,1,49.99
2023-12-04,ORD019,Paulo Santos,PROD123,5,499.95
2023-12-05,ORD020,Richard Roe,PROD456,2,99.98
2024-01-01,ORD021,Saanvi Sarkar,PROD789,3,149.97
2024-01-02,ORD022,Shirley Rodriguez,PROD123,1,99.99
2024-01-03,ORD023,Sofia Martinez,PROD456,4,199.96
2024-01-04,ORD024,Terry Whitlock,PROD789,2,99.98
2024-01-05,ORD025,Wang Xiulan,PROD123,3,299.97
```

Ce fichier contient des exemples de données de test à utiliser dans votre table DynamoDB au format CSV (valeurs séparées par des virgules) standard.

Script Python de chargement d'exemples de données

Copiez et collez le code suivant dans un fichier nommé `load_sample_data.py`.

```
import boto3
import csv
from decimal import Decimal

# Initialize the DynamoDB client
dynamodb = boto3.resource('dynamodb')
table = dynamodb.Table('MyOrderTable')
print("DDB client initialized.")

def load_data_from_csv(filename):
    with open(filename, 'r') as file:
        csv_reader = csv.DictReader(file)
        for row in csv_reader:
            item = {
                'Order_number': row['Order_number'],
                'Date': row['Date'],
                'CustomerName': row['CustomerName'],
                'ProductID': row['ProductID'],
                'Quantity': int(row['Quantity']),
                'TotalAmount': Decimal(str(row['TotalAmount']))
            }
            table.put_item(Item=item)
            print(f"Added item: {item['Order_number']} - {item['Date']}")

if __name__ == "__main__":
    load_data_from_csv('sample_data.csv')
```

```
    print("Data loading completed.")
```

Ce script Python utilise d'abord le AWS SDK pour Python (Boto3) pour créer une connexion à votre table DynamoDB. Il effectue ensuite une itération sur chaque ligne du fichier CSV de données d'exemple, crée un élément à partir de cette ligne et écrit l'élément dans la table DynamoDB à l'aide du kit SDK boto3.

Code de fonction Python

Copiez et collez le code suivant dans un fichier nommé `lambda_function.py`.

```
import boto3
from datetime import datetime, timedelta
from boto3.dynamodb.conditions import Key, Attr
import logging

logger = logging.getLogger()
logger.setLevel("INFO")

def lambda_handler(event, context):
    # Initialize the DynamoDB client
    dynamodb = boto3.resource('dynamodb')

    # Specify the table name
    table_name = 'MyOrderTable'
    table = dynamodb.Table(table_name)

    # Get today's date
    today = datetime.now()

    # Calculate the date one year ago
    one_year_ago = (today - timedelta(days=365)).strftime('%Y-%m-%d')

    # Scan the table using a global secondary index
    response = table.scan(
        IndexName='Date-index',
        FilterExpression='#date < :one_year_ago',
        ExpressionAttributeNames={
            '#date': 'Date'
        },
        ExpressionAttributeValues={
            ':one_year_ago': one_year_ago
        }
```

```
    )

     # Delete old items
    with table.batch_writer() as batch:
        for item in response['Items']:
            Order_number = item['Order_number']
            batch.delete_item(
                Key={
                    'Order_number': Order_number,
                    'Date': item['Date']
                }
            )
            logger.info(f'deleted order number {Order_number}')

    # Check if there are more items to scan
    while 'LastEvaluatedKey' in response:
        response = table.scan(
            IndexName='DateIndex',
            FilterExpression='#date < :one_year_ago',
            ExpressionAttributeNames={
                '#date': 'Date'
            },
            ExpressionAttributeValues={
                ':one_year_ago': one_year_ago
            },
            ExclusiveStartKey=response['LastEvaluatedKey']
        )

        # Delete old items
        with table.batch_writer() as batch:
            for item in response['Items']:
                batch.delete_item(
                    Key={
                        'Order_number': item['Order_number'],
                        'Date': item['Date']
                    }
                )

    return {
        'statusCode': 200,
        'body': 'Cleanup completed successfully'
    }
```

Le code de la fonction Python contient la fonction de gestion (`lambda_handler`) que Lambda exécute lorsque votre fonction est appelée.

Lorsque la fonction est invoquée par le EventBridge planificateur, il utilise le AWS SDK pour Python (Boto3) pour créer une connexion à la table DynamoDB sur laquelle la tâche de maintenance planifiée doit être effectuée. Il utilise ensuite la bibliothèque Python `datetime` pour calculer la date d'il y a un an, avant de rechercher dans la table les éléments plus anciens et de les supprimer.

Notez que les réponses issues des opérations de requête et d'analyse DynamoDB sont limitées à une taille d'au maximum 1 Mo. Si la réponse est supérieure à 1 Mo, DynamoDB pagine les données et renvoie un élément `LastEvaluatedKey` dans la réponse. Pour garantir que notre fonction traite tous les enregistrements de la table, nous vérifions la présence de cette clé et continuons à analyser la table à partir de la dernière position évaluée jusqu'à ce que toute la table ait été analysée.

`fichier manifeste requirements.txt`

Copiez et collez le code suivant dans un fichier nommé `requirements.txt`.

```
boto3
```

Dans cet exemple, le code de votre fonction n'a qu'une seule dépendance qui ne fait pas partie de la bibliothèque Python standard : le kit SDK pour Python (Boto3) que la fonction utilise pour analyser et supprimer des éléments de la table DynamoDB.

> **Note**
>
> Une version du kit SDK pour Python (Boto3) est incluse dans l'environnement d'exécution Lambda, de sorte que votre code s'exécute sans ajouter Boto3 au package de déploiement de votre fonction. Toutefois, pour garder le contrôle total des dépendances de votre fonction et éviter d'éventuels problèmes de désalignement de version, la bonne pratique pour Python consiste à inclure toutes les dépendances de fonction dans le package de déploiement de votre fonction. Pour en savoir plus, consultez the section called "Dépendances d'exécution dans Python".

AWS SAM modèle (application de maintenance planifiée)

Copiez et collez le code suivant dans un fichier nommé `template.yaml`.

```
AWSTemplateFormatVersion: '2010-09-09'
```

```
Transform: AWS::Serverless-2016-10-31
Description: SAM Template for Lambda function and EventBridge Scheduler rule

Resources:
  MyLambdaFunction:
    Type: AWS::Serverless::Function
    Properties:
      FunctionName: ScheduledDBMaintenance
      CodeUri: ./
      Handler: lambda_function.lambda_handler
      Runtime: python3.11
      Architectures:
        - x86_64
      Events:
        ScheduleEvent:
          Type: ScheduleV2
          Properties:
            ScheduleExpression: cron(0 3 1 * ? *)
            Description: Run on the first day of every month at 03:00 AM
      Policies:
        - CloudWatchLogsFullAccess
        - Statement:
            - Effect: Allow
              Action:
                - dynamodb:Scan
                - dynamodb:BatchWriteItem
              Resource: !Sub 'arn:aws:dynamodb:${AWS::Region}:${AWS::AccountId}:table/
MyOrderTable'

  LambdaLogGroup:
    Type: AWS::Logs::LogGroup
    Properties:
      LogGroupName: !Sub /aws/lambda/${MyLambdaFunction}
      RetentionInDays: 30

Outputs:
  LambdaFunctionName:
    Description: Lambda Function Name
    Value: !Ref MyLambdaFunction
  LambdaFunctionArn:
    Description: Lambda Function ARN
    Value: !GetAtt MyLambdaFunction.Arn
```

> **Note**
>
> AWS SAM les modèles utilisent une convention de dénomination standard `detemplate.yaml`. Dans cet exemple, vous disposez de deux fichiers modèles : l'un pour créer la base de données d'exemple et l'autre pour créer l'application elle-même. Enregistrez-les dans des sous-répertoires distincts dans votre dossier de projet.

Ce AWS SAM modèle définit les ressources de votre application. Nous définissons la fonction Lambda à l'aide de la ressource `AWS::Serverless::Function`. Le calendrier du EventBridge planificateur et le déclencheur permettant d'invoquer la fonction Lambda sont créés en utilisant la `Events` propriété de cette ressource en utilisant un type de. `ScheduleV2` Pour en savoir plus sur la définition des plannings du EventBridge planificateur dans les AWS SAM modèles, consultez ScheduleV2 dans le manuel du développeur.AWS Serverless Application Model

Outre la fonction Lambda et le calendrier du EventBridge planificateur, nous définissons également un groupe de CloudWatch journaux auquel votre fonction doit envoyer les enregistrements des éléments supprimés.

Script de test

Copiez et collez le code suivant dans un fichier nommé `test_app.py`.

```
import boto3
from datetime import datetime, timedelta
import json

# Initialize the DynamoDB client
dynamodb = boto3.resource('dynamodb')

# Specify your table name
table_name = 'YourTableName'
table = dynamodb.Table(table_name)

# Get the current date
current_date = datetime.now()

# Calculate the date one year ago
one_year_ago = current_date - timedelta(days=365)
```

```
# Convert the date to string format (assuming the date in DynamoDB is stored as a
 string)
one_year_ago_str = one_year_ago.strftime('%Y-%m-%d')

# Scan the table
response = table.scan(
    FilterExpression='#date < :one_year_ago',
    ExpressionAttributeNames={
        '#date': 'Date'
    },
    ExpressionAttributeValues={
        ':one_year_ago': one_year_ago_str
    }
)

# Process the results
old_records = response['Items']

# Continue scanning if we have more items (pagination)
while 'LastEvaluatedKey' in response:
    response = table.scan(
        FilterExpression='#date < :one_year_ago',
        ExpressionAttributeNames={
            '#date': 'Date'
        },
        ExpressionAttributeValues={
            ':one_year_ago': one_year_ago_str
        },
        ExclusiveStartKey=response['LastEvaluatedKey']
    )
    old_records.extend(response['Items'])

for record in old_records:
    print(json.dumps(record))

# The total number of old records should be zero.
print(f"Total number of old records: {len(old_records)}")
```

Ce script de test utilise le AWS SDK pour Python (Boto3) pour créer une connexion à votre table DynamoDB et rechercher les éléments datant de plus d'un an. Pour confirmer que la fonction Lambda s’est bien exécutée, à la fin du test, la fonction affiche le nombre d’enregistrements de plus d’un an encore présents dans la table. Si l’exécution de la fonction Lambda a réussi, le nombre d’anciens enregistrements dans la table doit être égal à zéro.

Création et remplissage de l’exemple de table DynamoDB

Pour tester votre application de maintenance planifiée, vous devez d’abord créer une table DynamoDB et la remplir avec des exemples de données. Vous pouvez créer le tableau manuellement à l’aide de l’ Console de gestion AWS ou en utilisant AWS SAM. Nous vous recommandons de l'utiliser AWS SAM pour créer et configurer rapidement le tableau à l'aide de quelques AWS CLI commandes.

Console

Créer le tableau DynamoDB

1. Ouvrez la page Tables (Tables) de la console DynamoDB.
2. Choisissez Créer un tableau.
3. Créez la table en procédant comme suit :
   a. Sous Détails de la table, dans Nom de la table, saisissez **`MyOrderTable`**.
   b. Pour Clé de partition, saisissez **`Order_number`**, et conservez le type défini sur Chaîne.
   c. Pour la Clé de tri, saisissez **`Date`** et conservez le type défini sur Chaîne.
   d. Laissez Paramètres du tableau définis sur Paramètres par défaut et choisissez Créer une table.
4. Lorsque la création de votre table est terminée et que son Statut affiche Actif, créez un index secondaire global (GSI) en procédant comme suit. Votre application utilise ce GSI pour rechercher des éléments directement par date afin de déterminer ceux à supprimer.
   a. MyOrderTableChoisissez dans la liste des tables.
   b. Choisissez l’onglet Index.
   c. Sous Index secondaires globaux, choisissez Créer un index.
   d. Sous Détails de l’index, saisissez **`Date`** la Clé de partition et laissez Type de données défini sur Chaîne.
   e. Pour Nom de l'index, saisissez **`Date-index`**.
   f. Laissez les valeurs par défaut de tous les autres paramètres, faites défiler l’écran vers le bas et choisissez Créer un index.

AWS SAM

Créer le tableau DynamoDB

1. Accédez au dossier dans lequel vous avez enregistré le fichier `template.yaml` de la table DynamoDB. Notez que cet exemple utilise deux fichiers `template.yaml`. Assurez-vous qu'ils sont enregistrés dans des sous-dossiers distincts et que vous vous trouvez dans le bon dossier contenant le modèle pour créer votre table DynamoDB.
2. Exécutez la commande suivante.

   ```
   sam build
   ```

   Cette commande rassemble les artefacts de création pour les ressources que vous souhaitez déployer et les place dans le format et l'emplacement appropriés pour les déployer.
3. Pour créer la ressource DynamoDB spécifiée dans le fichier `template.yaml`, exécutez la commande suivante.

   ```
   sam deploy --guided
   ```

   L'utilisation du `--guided` drapeau signifie qu'il AWS SAM affiche des instructions pour vous guider tout au long du processus de déploiement. Pour ce déploiement, définissez `Stack name` sur **`cron-app-test-db`** et acceptez les valeurs par défaut pour toutes les autres options à l'aide de la touche Entrée.

   Une AWS SAM fois la création de la ressource DynamoDB terminée, le message suivant devrait s'afficher.

   ```
   Successfully created/updated stack - cron-app-test-db in us-west-2
   ```
4. Vous pouvez également vérifier que la table DynamoDB a été créée en ouvrant la page Tables de la console DynamoDB. Vous devriez voir une table nommée `MyOrderTable`.

Après avoir créé votre table, vous devez ensuite ajouter des exemples de données pour tester votre application. Le fichier CSV `sample_data.csv` que vous avez téléchargé précédemment contient un certain nombre d'exemples d'entrées comprenant des numéros de commande, des dates et des informations sur les clients et les commandes. Utilisez le script python `load_sample_data.py` fourni pour ajouter ces données à votre table.

Pour ajouter les exemples de données à la table

1. Naviguez jusqu'au répertoire contenant les fichiers `sample_data.csv` et `load_sample_data.py`. Si ces fichiers se trouvent dans des répertoires distincts, déplacez-les afin qu'ils soient enregistrés au même endroit.
2. Créez un environnement virtuel Python dans lequel exécuter le script en exécutant la commande suivante. Nous vous recommandons d'utiliser un environnement virtuel, car lors de l'étape suivante, vous devrez installer l' AWS SDK pour Python (Boto3).

   ```
   python -m venv venv
   ```

3. Activez l'environnement virtuel en exécutant la commande suivante.

   ```
   source venv/bin/activate
   ```

4. Installez le kit SDK for Python (Boto3) dans votre environnement virtuel en exécutant la commande suivante. Le script utilise cette bibliothèque pour se connecter à votre table DynamoDB et ajouter les éléments.

   ```
   pip install boto3
   ```

5. Exécutez le script pour remplir la table en exécutant la commande suivante.

   ```
   python load_sample_data.py
   ```

   Si le script s'exécute correctement, il doit afficher chaque élément sur la console au fur et à mesure du chargement et du rapport `Data loading completed`.
6. Désactivez l'environnement virtuel en exécutant la commande suivante.

   ```
   deactivate
   ```

7. Vous pouvez vérifier que les données ont été chargées dans votre table DynamoDB en procédant comme suit :

   a. Ouvrez la page Explorer les éléments de la console DynamoDB et sélectionnez votre table (`MyOrderTable`).

   b. Dans le volet Éléments renvoyés, vous devriez voir les 25 éléments du fichier CSV que le script a ajouté à la table.

Création de l’application de maintenance planifiée

Vous pouvez créer et déployer les ressources pour cet exemple d'application étape par étape en utilisant Console de gestion AWS ou en utilisant AWS SAM. Dans un environnement de production, nous vous recommandons d'utiliser un outil Infrustracture-as-Code (iAc) permettant de déployer de manière répétitive des applications sans serveur sans recourir AWS SAM à des processus manuels.

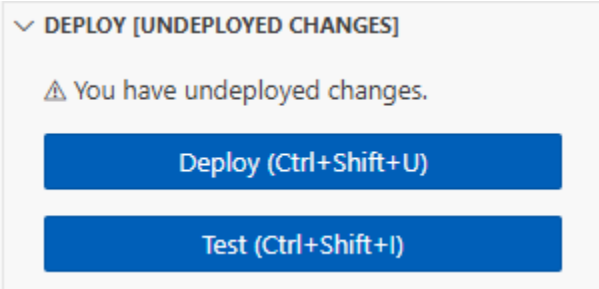
Pour cet exemple, suivez les instructions de la console pour savoir comment configurer chaque AWS ressource séparément, ou suivez les AWS SAM instructions pour déployer rapidement l'application à l'aide de AWS CLI commandes.

Console

Pour créer la fonction à l'aide du Console de gestion AWS

Créez d’abord une fonction contenant le code de démarrage de base. Vous remplacez ensuite ce code par votre propre code de fonction en copiant et collant le code directement dans l’éditeur de code Lambda ou en chargeant votre code en tant que package `.zip`. Pour cette tâche, nous vous recommandons de copier-coller le code.

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez Create Event Function.
3. Choisissez Créer à partir de zéro.
4. Sous Informations de base, procédez comme suit :
   a. Sous Nom de la fonction, saisissez **`ScheduledDBMaintenance`**.
   b. Pour Environnement d’exécution, choisissez la dernière version de Python.
   c. Pour Architecture, choisissez x86_64.
5. Choisissez Create Event Function.
6. Une fois votre fonction créée, vous pouvez la configurer à l’aide du code de fonction fourni.
   a. Dans le volet Source du code, remplacez le code Hello world créé par Lambda par le code de fonction Python du fichier `lambda_function.py` que vous avez enregistré précédemment.
   b. Dans la section DÉPLOYER, choisissez Déployer pour mettre à jour le code de votre fonction :



Pour configurer la mémoire et le délai d'expiration d'une fonction (console)

1. Sélectionnez l'onglet Configuration correspondant à votre fonction.
2. Dans le volet de Configuration générale, choisissez Modifier.
3. Réglez Mémoire sur 256 Mo et Délai d'expiration sur 15 secondes. Si vous traitez une table volumineuse contenant de nombreux enregistrements, par exemple dans le cas d'un environnement de production, vous pouvez envisager de définir un délai d'expiration plus élevé. Cela donne à votre fonction plus de temps pour scanner et nettoyer la base de données.
4. Cliquez sur Enregistrer.

Pour configurer le format de journal (console)

Vous pouvez configurer les fonctions Lambda pour générer des journaux au format texte non structuré ou au format JSON. Nous vous recommandons d'utiliser le format JSON pour les journaux afin de faciliter la recherche et le filtrage des données de journal. Pour en savoir plus sur les options de configuration du journal Lambda, consultez the section called "Configuration de contrôles de journalisation avancés pour les fonctions d'événement Lambda".

1. Sélectionnez l'onglet Configuration correspondant à votre fonction.
2. Sélectionnez Outils de surveillance et d'exploitation.
3. Dans le volet de configuration de la journalisation, choisissez Modifier.
4. Pour Configuration de journalisation, sélectionnez JSON.
5. Cliquez sur Enregistrer.

Pour configurer les autorisations IAM

Pour donner à votre fonction les autorisations nécessaires pour lire et supprimer des éléments DynamoDB, vous devez ajouter une politique au rôle d'exécution de votre fonction définissant les autorisations nécessaires.

1. Ouvrez l'onglet Configuration, puis choisissez Autorisations dans la barre de navigation de gauche.
2. Sous Rôle d'exécution, choisissez le nom du rôle.
3. Dans la console IAM, choisissez Ajouter des autorisations, puis Créer une politique intégrée.
4. Utilisez l'éditeur JSON et saisissez la politique suivante :

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "dynamodb:Scan",
                "dynamodb:DeleteItem",
                "dynamodb:BatchWriteItem"
            ],
            "Resource": "arn:aws:dynamodb:*:*:table/MyOrderTable"
        }
    ]
}
```

5. Nommez la politique **`DynamoDBCleanupPolicy`**, puis créez-la.

Pour configurer le EventBridge planificateur en tant que déclencheur (console)

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez votre fonction (`ScheduledDBMaintenance`).
3. Dans le volet de Présentation de la fonction, choisissez Ajouter un déclencheur.
4. Dans la liste déroulante des sources de déclenchement, choisissez Scheduler.
5. Configurez la planification en procédant comme suit :

    a. Dans le champ Nom du calendrier, entrez**`DynamoDBCleanupSchedule`**.

b. Pour le groupe Schedule, laissez la valeur par défaut (`default`).

c. Pour le type de planification, choisissez Planification récurrente et entrez l'expression cron suivante :**`cron(0 3 1 * ? *)`**.

   Lorsqu'elle est évaluée, cette expression cron s'exécute le premier jour de chaque mois à 03h00.

d. Pour la fenêtre horaire flexible, sélectionnez Désactivé.

e. Laissez le champ Charge utile vide.

f. Pour le rôle d'exécution, choisissez Créer un nouveau rôle pour cette planification et entrez un nom de rôle. EventBridge Le planificateur crée une nouvelle politique avec les autorisations requises dont le planning a besoin pour appeler votre fonction.

6. Choisissez Ajouter.

AWS SAM

Pour déployer l'application à l'aide de AWS SAM

1. Accédez au dossier dans lequel vous avez enregistré le fichier `template.yaml` de l'application. Notez que cet exemple utilise deux fichiers `template.yaml`. Assurez-vous qu'ils sont enregistrés dans des sous-dossiers distincts et que vous vous trouvez dans le bon dossier contenant le modèle pour créer l'application.
2. Copiez les fichiers `lambda_function.py` et `requirements.txt` que vous avez téléchargés précédemment dans le même dossier. L'emplacement du code spécifié dans le AWS SAM modèle est`./`, c'est-à-dire l'emplacement actuel. AWS SAM recherche dans ce dossier le code de la fonction Lambda lorsque vous essayez de déployer l'application.
3. Exécutez la commande suivante.

   ```
   sam build --use-container
   ```

   Cette commande rassemble les artefacts de création pour les ressources que vous souhaitez déployer et les place dans le format et l'emplacement appropriés pour les déployer. La spécification de l'`--use-container`option crée votre fonction dans un conteneur Lambda-like Docker. Nous l'utilisons ici, vous n'avez donc pas besoin d'installer Python 3.12 sur votre machine locale pour que la compilation fonctionne.

4. Pour créer les ressources Lambda et EventBridge Scheduler spécifiées dans le `template.yaml` fichier, exécutez la commande suivante.

   ```
   sam deploy --guided
   ```

   L'utilisation du `--guided` drapeau signifie qu'il AWS SAM affiche des instructions pour vous guider tout au long du processus de déploiement. Pour ce déploiement, définissez `Stack name` sur **`cron-maintenance-app`** et acceptez les valeurs par défaut pour toutes les autres options à l'aide de la touche Entrée.

   Lorsque vous aurez AWS SAM terminé de créer les ressources Lambda et EventBridge Scheduler, le message suivant devrait s'afficher.

   ```
   Successfully created/updated stack - cron-maintenance-app in us-west-2
   ```

5. Vous pouvez également vérifier que la fonction Lambda a été créée en ouvrant la page Fonctions de la console Lambda. Vous devriez voir une fonction nommée `ScheduledDBMaintenance`.

Test de l'application

Pour vérifier que votre planification déclenche correctement votre fonction et que celle-ci nettoie correctement les enregistrements de la base de données, vous pouvez modifier temporairement votre planification pour qu'elle ne s'exécute qu'une seule fois à une heure précise. Vous pouvez ensuite exécuter à nouveau `sam deploy` pour réinitialiser votre planification récurrente afin qu'elle s'exécute une fois par mois.

Pour exécuter l'application à l'aide du Console de gestion AWS

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez votre fonction (`ScheduledDBMaintenance`).
3. Dans la section Déclencheurs, choisissez le `DynamoDBCleanupSchedule` déclencheur.
4. Choisissez Modifier.
5. Pour le type de planification, choisissez One-time planification.
6. Réglez votre durée d'invocation sur quelques minutes, puis choisissez Enregistrer.

Une fois la planification exécutée et sa cible invoquée, vous exécutez le script `test_app.py` pour vérifier que votre fonction a bien supprimé tous les anciens enregistrements de la table DynamoDB.

Pour vérifier que les anciens enregistrements sont supprimés à l'aide d'un script Python

1. Dans votre ligne de commande, accédez au dossier dans lequel vous avez enregistré `test_app.py`.
2. Exécutez le script.

   ```
   python test_app.py
   ```

   En cas de réussite, le résultat suivant s'affiche.

   ```
   Total number of old records: 0
   ```

Étapes suivantes

Vous pouvez désormais modifier le calendrier du EventBridge planificateur pour répondre aux exigences spécifiques de votre application. EventBridge Le planificateur prend en charge les expressions de planification suivantes : cron, rate et plannings ponctuels.

Pour plus d'informations sur les expressions de planification du EventBridge planificateur, consultez la section Types de planification dans le guide de l'utilisateur du EventBridge planificateur. Gestion des accès dans le guide de l'utilisateur IAM

Langages de programmation

Les fonctions d'événement Lambda (anciennement connues sous le nom de fonctions Lambda) prennent en charge un large éventail de langages de programmation courants. Chacun possède une expérience de programmation idiomatique adaptée à ce langage.

Chaque langage de programmation est pris en charge par un environnement d'exécution correspondant, qui fournit l'environnement d'exécution spécifique au langage pour votre fonction.

- the section called “Construire avec Node.js”
- the section called “Construire avec TypeScript”
- the section called “Création avec Python”

- the section called “Création avec Ruby”
- the section called “Création avec Java”
- the section called “Création avec Go”
- the section called “Création avec C#”
- the section called “Construire avec PowerShell”
- the section called “Création avec Rust”

Création de fonctions événementielles Lambda avec Node.js

Tu peux courir JavaScript code avec Node.js dans AWS Lambda Fonctions événementielles. Lambda fournit temps d'exécution pour Node.js qui exécutent votre code pour traiter les événements. Votre code s'exécute dans un environnement qui inclut le AWS SDK pour JavaScript, avec les informations d'identification d'un Gestion des identités et des accès AWS rôle (IAM) que vous gérez. Pour en savoir plus sur les versions du SDK incluses dans le Node.js temps d'exécution, voir the section called “Runtime-included Versions du SDK”.

Lambda prend en charge les éléments suivants Node.js temps d'exécution.

Nom	Identifiant	Système d’exploitation	Date d’obsolescence	Créer la fonction de blocage	Mettre à jour la fonction de blocage
Node.js 26	`nodejs26.x`	Amazon Linux 2	Non planifié	Non planifié	Non planifié
Node.js 24	`nodejs24.x`	Amazon Linux 2	30 avril 2028	1 juin 2028	1 juillet 2028
Node.js 22	`nodejs22.x`	Amazon Linux 2	30 avril 2027	29 juillet 2027	31 août 2027

Pour créer un Node.js Fonction événementielle

1. Ouvrez la console Lambda.
2. Choisissez Créer une fonction d'événement.

3. Configurez les paramètres suivants :
   - Nom de la fonction : saisissez le nom de la fonction.
   - Temps d'exécution: Choisissez Node.js 24. x.
4. Choisissez Créer une fonction d'événement.

La console crée une fonction événementielle Lambda avec un seul fichier source nommé `index.mjs`. Vous pouvez modifier ce fichier et ajouter d'autres fichiers dans l'éditeur de code intégré. Dans la section DÉPLOYER, choisissez Déployer pour mettre à jour le code de votre fonction. Ensuite, pour exécuter votre code, choisissez Créer un événement de test dans la section ÉVÉNEMENTS DE TEST.

Le fichier `index.mjs` exporte une fonction nommée `handler` qui accepte un objet événement et un objet contexte. Il s'agit de la fonction de gestionnaire que Lambda appelle lors de l'invocation de la fonction. Le Node.js function runtime obtient les événements d'invocation de Lambda et les transmet au gestionnaire. Dans la configuration de fonction, la valeur de gestionnaire est `index.handler`.

Lorsque vous enregistrez votre code de fonction, la console Lambda crée un package de déploiement d'archive de fichiers .zip. Lorsque vous développez votre code de fonction en dehors de la console (à l'aide d'un IDE), vous devez créer un package de déploiement pour charger votre code dans la fonction Lambda.

Le runtime de la fonction transmet un objet de contexte au gestionnaire, en plus de l'événement d'invocation. L'objet de contexte contient des informations supplémentaires sur l'invocation, la fonction et l'environnement d'exécution. Des informations supplémentaires sont disponibles dans les variables d'environnement.

Votre fonction Lambda est fournie avec CloudWatch Groupe de journaux. L'exécution de la fonction envoie les détails de chaque appel à CloudWatch Journaux. Il relaie tous les journaux que votre fonction génère pendant l'invocation. Si votre fonction renvoie une erreur, Lambda met en forme l'erreur et la renvoie à l'appelant.

Rubriques

- Runtime-included Versions du SDK
- Utilisation de keep-alive pour les connexions TCP
- Chargement des certificats CA
- Expérimental Node.js fonctionnalités

- Définissez le gestionnaire de fonctions d'événement Lambda dans Node.js
- Déployez les fonctions d'événement Node.js Lambda avec des archives de fichiers .zip
- Déployer des fonctions d'événement Node.js Lambda avec des images de conteneur
- Utilisation de couches pour les fonctions d' Node.js événement Lambda
- Utilisation de l'objet de contexte Lambda pour récupérer les informations de la fonction Node.js d'événement
- Enregistrez et surveillez les fonctions des Node.js événements Lambda
- Instrumentation du Node.js code dans AWS Lambda

Runtime-included Versions du SDK

Tous Lambda pris en charge Node.js temps d'exécution inclure une version mineure spécifique du AWS SDK pour JavaScript v3, pas le dernière version. La version mineure spécifique incluse dans l'environnement d'exécution dépend de la version de l'environnement d'exécution et de votre Région AWS. Pour trouver la version spécifique du SDK incluse dans l'environnement d'exécution que vous utilisez, créez une fonction événementielle Lambda avec le code suivant.

Example index.mjs

```
import packageJson from '@aws-sdk/client-s3/package.json' with { type: 'json' };

export const handler = async () => ({ version: packageJson.version });
```

Ceci renvoie une réponse au format suivant :

```
{
  "version": "3.632.0"
}
```

Pour plus d'informations, consultez Utilisation du SDK pour la JavaScript version 3 dans votre gestionnaire.

Utilisation de keep-alive pour les connexions TCP

La valeur par défaut Node.js HTTP/HTTPS l'agent crée une nouvelle connexion TCP pour chaque nouvelle demande. Pour éviter les coûts liés à l'établissement de nouvelles connexions, keep-alive

est activé par défaut dans tous prise en charge Node.js temps d'exécution. Keep-alive peut réduire les temps de requête pour les fonctions Lambda qui effectuent plusieurs appels d'API à l'aide du SDK.

Pour désactiver keep-alive, voir Réutiliser les connexions avec keep-alive in Node.js dans le AWS SDK pour JavaScript Guide du développeur 3.x. Pour plus d'informations sur l'utilisation de keep-alive, voir HTTP keep-alive est activé par défaut dans le mode modulaire AWS SDK pour JavaScript sur le AWS Blog sur les outils pour développeurs.

Chargement des certificats CA

Pour Node.js versions d'exécution jusqu'à Node.js 18, Lambda se charge automatiquement Amazon-specific des certificats CA (autorité de certification) pour vous permettre de créer plus facilement des fonctions qui interagissent avec d'autres Services AWS. Par exemple, Lambda inclut les certificats Amazon RDS nécessaires pour valider le certificat d'identité du serveur installé sur votre base de données Amazon RDS. Ce comportement peut avoir un impact sur les performances lors des démarrages à froid.

Commençant par Node.js 20, Lambda ne charge plus de certificats CA supplémentaires par défaut. Le Node.js L'environnement d'exécution 2.0 contient un fichier de certificat contenant tous les certificats Amazon CA situés à l'adresse `/var/runtime/ca-cert.pem`. Pour rétablir le même comportement à partir de Node.js 18 environnements d'exécution et versions antérieures, définissez `NODE_EXTRA_CA_CERTS` variable d'environnement pour `/var/runtime/ca-cert.pem`.

Pour des performances optimales, nous vous recommandons de regrouper uniquement les certificats dont vous avez besoin avec votre package de déploiement et de les charger via le `NODE_EXTRA_CA_CERTS` variable d'environnement. Le fichier de certificats doit être composé d'un ou de plusieurs certificats d'autorité de certification racine ou intermédiaire sécurisés au format PEM. Par exemple, pour RDS, incluez les certificats requis à côté de votre code en tant que `certificates/rds.pem`. Chargez ensuite les certificats en réglant `NODE_EXTRA_CA_CERTS` sur `/var/task/certificates/rds.pem`.

Expérimental Node.js fonctionnalités

L'amont Node.js les versions linguistiques activent certaines fonctionnalités expérimentales par défaut. Lambda désactive ces fonctionnalités pour garantir la stabilité de l'exécution et des performances constantes. Le tableau suivant répertorie les fonctionnalités expérimentales désactivées par Lambda.

Fonctionnalité expérimentale	Supporté Node.js versions	Node.js drapeau appliqué par Lambda	Indicateur Lambda à réactiver
Prise en charge de l'importation de modules à l'aide de require dans les modules ES	Node.js 20, Node.js 22, Node.js 24	`--no-experimental-require-module`	`--experimental-require-module`
Prise en charge de la détection automatique des modules ES par rapport aux modules CommonJS	Node.js 22, Node.js 24	`--no-experimental-detect-module`	`--experimental-detect-module`

Pour activer une fonctionnalité expérimentale désactivée, définissez l'indicateur de réactivation dans la variable d'environnement `NODE_OPTIONS`. Par exemple, pour activer la prise en charge de require dans les modules ES, réglez `NODE_OPTIONS` sur `--experimental-require-module`. Lambda détecte ce remplacement et supprime l'indicateur de désactivation correspondant.

> **Important**
>
> L'utilisation de fonctionnalités expérimentales peut entraîner des problèmes d'instabilité et de performance. Ces fonctionnalités peuvent être modifiées ou supprimées à l'avenir Node.js versions. Les fonctions qui utilisent des fonctionnalités expérimentales ne sont pas éligibles au contrat de niveau de service (SLA) Lambda ou à AWS Support

Définissez le gestionnaire de fonctions d'événement Lambda dans Node.js

Le gestionnaire de fonctions d'événement Lambda est la méthode de votre code de fonction qui traite les événements. Lorsque votre fonction est invoquée, Lambda exécute la méthode du gestionnaire. Votre fonction s'exécute jusqu'à ce que le gestionnaire renvoie une réponse, se ferme ou expire.

Cette page explique comment utiliser les gestionnaires de fonctions d'événement Lambda dans Node.js, notamment les options de configuration du projet, les conventions de dénomination et les meilleures pratiques. Cette page inclut également un exemple de fonction Node.js Lambda qui collecte des informations relatives à une commande, produit un reçu sous forme de fichier texte et place ce fichier dans un bucket Amazon Simple Storage Service (Amazon S3). Pour plus d'informations sur le déploiement de votre fonction après l'avoir écrite, consultez the section called "Déploiement d'archives de fichiers .zip" ou the section called "Déploiement d'images de conteneur".

Rubriques

- Configuration de votre projet Node.js de gestionnaire
- Exemple de code de fonction d'événement Node.js Lambda
- Modules CommonJS et ES
- Node.js initialisation
- Convention de nommage du gestionnaire
- Définition et accès à l'objet d'événement d'entrée
- Modèles de gestionnaire valides pour les fonctions Node.js
- Utilisation du SDK pour la JavaScript version 3 dans votre gestionnaire
- Accès aux variables d'environnement
- Utilisation de l'état global
- Meilleures pratiques en matière de code pour les Node.js fonctions d'événement Lambda

Configuration de votre projet Node.js de gestionnaire

Il existe plusieurs manières d'initialiser un projet Node.js Lambda. Par exemple, vous pouvez créer un Node.js projet standard en utilisant`npm`, créer une AWS SAM application ou créer une AWS CDK application.

Pour créer le projet avec `npm` :

```
npm init
```

Cette commande initialise votre projet et génère un fichier `package.json` qui gère les métadonnées et dépendances de votre projet.

Le code de votre fonction se trouve dans un `.mjs` JavaScript fichier `.js` or. Dans l'exemple suivant, nous nommons ce fichier `index.mjs`, car il utilise un gestionnaire de modules ES. Lambda prend en charge à la fois le module ES et les gestionnaires CommonJS. Pour plus d'informations, consultez Modules CommonJS et ES.

Un projet de fonction Node.js Lambda typique suit cette structure générale :

```
/project-root
  ### index.mjs – Contains main handler
  ### package.json – Project metadata and dependencies
  ### package-lock.json – Dependency lock file
  ### node_modules/ – Installed dependencies
```

Exemple de code de fonction d'événement Node.js Lambda

L'exemple de code de fonction Lambda suivant prend en compte les informations relatives à une commande, produit un reçu sous forme de fichier texte et place ce fichier dans un compartiment Amazon S3.

Example Fonction d'événement Lambda index.mjs

```
import { S3Client, PutObjectCommand } from '@aws-sdk/client-s3';

// Initialize the S3 client outside the handler for reuse
const s3Client = new S3Client();

/**
 * Lambda handler for processing orders and storing receipts in S3.
 * @param {Object} event - Input event containing order details
 * @param {string} event.order_id - The unique identifier for the order
 * @param {number} event.amount - The order amount
 * @param {string} event.item - The item purchased
 * @returns {Promise<string>} Success message
 */
export const handler = async(event) => {
    try {
        // Access environment variables
        const bucketName = process.env.RECEIPT_BUCKET;
```

```
        if (!bucketName) {
            throw new Error('RECEIPT_BUCKET environment variable is not set');
        }

        // Create the receipt content and key destination
        const receiptContent = `OrderID: ${event.order_id}\nAmount: $
${event.amount.toFixed(2)}\nItem: ${event.item}`;
        const key = `receipts/${event.order_id}.txt`;

        // Upload the receipt to S3
        await uploadReceiptToS3(bucketName, key, receiptContent);

        console.log(`Successfully processed order ${event.order_id} and stored receipt
 in S3 bucket ${bucketName}`);
        return 'Success';
    } catch (error) {
        console.error(`Failed to process order: ${error.message}`);
        throw error;
    }
};

/**
 * Helper function to upload receipt to S3
 * @param {string} bucketName - The S3 bucket name
 * @param {string} key - The S3 object key
 * @param {string} receiptContent - The content to upload
 * @returns {Promise<void>}
 */
async function uploadReceiptToS3(bucketName, key, receiptContent) {
    try {
        const command = new PutObjectCommand({
            Bucket: bucketName,
            Key: key,
            Body: receiptContent
        });

        await s3Client.send(command);
    } catch (error) {
        throw new Error(`Failed to upload receipt to S3: ${error.message}`);
    }
}
```

Ce fichier `index.mjs` comprend les sections suivantes :

- Bloc `import` : utilisez ce bloc pour inclure les bibliothèques que votre fonction Lambda requiert, comme les clients du SDK AWS.
- Déclaration `const s3Client` : initialise un client Amazon S3 en dehors de la fonction du gestionnaire. Lambda exécute donc ce code pendant la phase d'initialisation, et le client est conservé pour être réutilisé lors de plusieurs appels.
- Bloc de commentaires JSDoc : définissez les types d'entrée et de sortie pour votre gestionnaire à l'aide d'annotations JSDoc.
- `export const handler` : le gestionnaire de la fonction principal que Lambda invoque. Lorsque vous déployez votre fonction, spécifiez `index.handler` pour la propriété Gestionnaire. La valeur de la propriété `Handler` est le nom du fichier et le nom de la méthode du gestionnaire exporté, séparés par un point.
- Fonction `uploadReceiptToS3` : une fonction d'assistance référencée par la fonction du gestionnaire principal.

Pour que cette fonction fonctionne correctement, son rôle d'exécution doit autoriser l'action `s3:PutObject`. Assurez-vous également de définir la variable d'environnement `RECEIPT_BUCKET`. Après une invocation réussie, le compartiment Amazon S3 doit contenir un fichier de reçu.

Modules CommonJS et ES

Node.js prend en charge deux systèmes de modules : les modules CommonJS et ECMAScript (modules ES). Lambda recommande d'utiliser les modules ES car ils prennent en charge l'attente de haut niveau, ce qui permet d'effectuer des tâches asynchrones lors de l'initialisation de l'environnement d'exécution.

Node.js traite les fichiers avec une extension de nom de `.cjs` fichier comme des modules CommonJS tandis qu'une `.mjs` extension désigne les modules ES. Par défaut, Node.js traite les fichiers portant l'extension de nom de `.js` fichier comme des modules CommonJS. Vous pouvez configurer Node.js pour traiter les `.js` fichiers comme des modules ES en spécifiant le `type` as `module` dans le `package.json` fichier de la fonction. Vous pouvez configurer Node.js Lambda pour détecter automatiquement si un `.js` fichier doit être traité comme CommonJS ou comme un module ES en ajoutant l'`–experimental-detect-module`indicateur à la `NODE_OPTIONS` variable d'environnement. Pour plus d'informations, consultez la section Node.js Fonctionnalités expérimentales.

Les exemples suivants montrent des gestionnaires de fonctions écrits à l'aide de modules ES et de modules CommonJS. Les autres exemples de cette page utilisent tous des modules ES.

ES module example

Example– Gestionnaire de modules ES

```
const url = "https://aws.amazon.com/";

export const handler = async(event) => {
    try {
        const res = await fetch(url);
        console.info("status", res.status);
        return res.status;
    }
    catch (e) {
        console.error(e);
        return 500;
    }
};
```

CommonJS module example

Example– Gestionnaire de modules CommonJS

```
const https = require("https");
let url = "https://aws.amazon.com/";

exports.handler = async function (event) {
  let statusCode;
  await new Promise(function (resolve, reject) {
    https.get(url, (res) => {
        statusCode = res.statusCode;
        resolve(statusCode);
      }).on("error", (e) => {
        reject(Error(e));
      });
  });
  console.log(statusCode);
  return statusCode;
};
```

Node.js initialisation

Node.js utilise un I/O modèle non bloquant qui prend en charge des opérations asynchrones efficaces à l'aide d'une boucle d'événements. Par exemple, si elle Node.js effectue un appel réseau, la fonction continue de traiter d'autres opérations sans bloquer une réponse réseau. Lorsque la réponse du réseau est reçue, elle est placée dans la file de rappel. Les tâches de la file d'attente sont traitées lorsque la tâche en cours est terminée.

Lambda recommande d'utiliser l'attente de haut niveau afin que les tâches asynchrones initiées lors de l'initialisation de l'environnement d'exécution soient terminées pendant l'initialisation. Les tâches asynchrones qui ne sont pas terminées lors de l'initialisation sont généralement exécutées lors de la première invocation de la fonction. Cela peut entraîner un comportement inattendu ou des erreurs.

Par exemple, l'initialisation de votre fonction peut effectuer un appel réseau pour récupérer un paramètre depuis le Parameter Store AWS . Si cette tâche n'est pas terminée lors de l'initialisation, la valeur peut être nulle lors d'un appel. Il peut également y avoir un délai entre l'initialisation et l'appel, ce qui peut déclencher des erreurs lors d'opérations sensibles au facteur temps. En particulier, les appels de AWS service peuvent s'appuyer sur des signatures de demande urgentes, ce qui entraîne l'échec des appels de service si l'appel n'est pas terminé pendant la phase d'initialisation.

L'exécution des tâches lors de l'initialisation améliore généralement les performances de démarrage à froid et les performances d'appel d'abord lors de l'utilisation de la concurrence provisionnée. Pour plus d'informations, consultez notre article de blog Using Node.js ES modules and top-level await in AWS Lambda.

Convention de nommage du gestionnaire

Lorsque vous configurez une fonction, la valeur du paramètre Gestionnaire est le nom du fichier et le nom de la méthode du gestionnaire exporté, séparés par un point. La valeur par défaut des fonctions créées dans la console et dans les exemples de ce guide est `index.handler`. Cela indique la méthode `handler` qui est exportée à partir du fichier `index.js` ou `index.mjs`.

Si vous créez une fonction dans la console en utilisant un nom de fichier ou un nom de gestionnaire de fonction différent, vous devez modifier le nom du gestionnaire par défaut.

Pour modifier le nom du gestionnaire de fonction (console)

1. Ouvrez la page Fonctions de la console Lambda et choisissez votre fonction.
2. Cliquez sur l’onglet Code.

3. Faites défiler l'écran jusqu'au volet Paramètres d'exécution et choisissez Modifier.
4. Dans Gestionnaire, saisissez le nouveau nom de votre gestionnaire de fonction.
5. Cliquez sur Enregistrer.

Définition et accès à l'objet d'événement d'entrée

JSON est le format d'entrée le plus courant et standard pour les fonctions Lambda. Dans cet exemple, la fonction exige une entrée similaire à l'exemple suivant :

```
{
    "order_id": "12345",
    "amount": 199.99,
    "item": "Wireless Headphones"
}
```

Lorsque vous utilisez des fonctions Lambda dans Node.js, vous pouvez définir la forme attendue de l'événement d'entrée à l'aide des annotations JSDoc. Dans cet exemple, nous définissons la structure d'entrée dans le commentaire JSDoc du gestionnaire :

```
/**
 * Lambda handler for processing orders and storing receipts in S3.
 * @param {Object} event - Input event containing order details
 * @param {string} event.order_id - The unique identifier for the order
 * @param {number} event.amount - The order amount
 * @param {string} event.item - The item purchased
 * @returns {Promise<string>} Success message
 */
```

Après avoir défini ces types dans votre commentaire JSDoc, vous pouvez accéder aux champs de l'objet d'événement directement dans votre code. Par exemple, `event.order_id` récupère la valeur de `order_id` à partir de l'entrée d'origine.

Modèles de gestionnaire valides pour les fonctions Node.js

Nous vous recommandons de l'utiliser async/awaitpour déclarer le gestionnaire de fonctions au lieu d'utiliser des rappels. Async/await est un moyen concis et lisible d'écrire du code asynchrone, sans avoir besoin de rappels imbriqués ou de promesses enchaînées. Avec async/await, vous pouvez écrire du code qui se lit comme du code synchrone, tout en étant asynchrone et non bloquant.

gestionnaires de fonctions asynchrones (recommandé)

Le mot-clé `async` marque une fonction comme étant asynchrone, et le mot-clé `await` met en pause l'exécution de la fonction jusqu'à ce qu'une `Promise` soit résolue. Le gestionnaire accepte les arguments suivants :

- `event` : contient les données d'entrée transmises à votre fonction.
- `context` : contient des informations sur l'invocation, la fonction et l'environnement d'exécution. Pour plus d'informations, consultez Utilisation de l'objet de contexte Lambda pour récupérer les informations de la fonction Node.js d'événement.

Voici les signatures valides pour le async/await modèle :

```
export const handler = async (event) => { };
```

```
export const handler = async (event, context) => { };
```

Gestionnaires de fonctions synchrones

Lorsque votre fonction n'exécute aucune tâche asynchrone, vous pouvez utiliser un gestionnaire de fonctions synchrones en utilisant l'une des signatures de fonction suivantes :

```
export const handler = (event) => { };
```

```
export const handler = (event, context) => { };
```

Gestionnaires de fonctions de diffusion des réponses

Lambda prend en charge le streaming de réponses avec. Node.js Les gestionnaires de fonctions de streaming de réponses utilisent le `awslambda.streamifyResponse()` décorateur et prennent 3 paramètres : `eventresponseStream`, et. `context` La signature de la fonction est la suivante :

```
export const handler = awslambda.streamifyResponse(async (event, responseStream,
 context) => { });
```

Pour plus d'informations, consultez Streaming de réponses pour les fonctions d'événement Lambda.

Callback-based gestionnaires de fonctions

> **Note**
>
> Callback-based les gestionnaires de fonctions ne sont pris en charge que jusqu'à Node.js 22. À partir de Node.js 24, les tâches asynchrones doivent être implémentées à l'aide de gestionnaires de fonctions asynchrones.

Callback-based les gestionnaires de fonctions doivent utiliser les arguments d'événement, de contexte et de rappel. Exemple :

```
export const handler = (event, context, callback) => { };
```

La fonction de rappel attend une réponse `Error` et une réponse, qui doit être JSON-serializable. La fonction continue à s'exécuter jusqu'à ce que la boucle d'événement soit vide ou que la fonction s'arrête. La réponse n'est pas envoyée à l'appelant tant que toutes les tâches d'événement de boucle ne sont pas terminées. Si la fonction expire, une erreur est renvoyée à la place. Vous pouvez configurer le moteur d'exécution pour envoyer la réponse immédiatement en attribuant à context.callback WaitsForEmptyEventLoop la valeur false.

Example– Requête HTTP avec callback

L'exemple suivant vérifie la fonction d'une URL et renvoie le code de statut au mécanisme d'appel.

```
import https from "https";
let url = "https://aws.amazon.com/";

export const handler = (event, context, callback) => {
  https.get(url, (res) => {
    callback(null, res.statusCode);
  }).on("error", (e) => {
    callback(Error(e));
  });
};
```

Utilisation du SDK pour la JavaScript version 3 dans votre gestionnaire

Vous utiliserez souvent les fonctions Lambda pour interagir avec d'autres AWS ressources ou pour les mettre à jour. Le moyen le plus simple d'interagir avec ces ressources est d'utiliser AWS SDK

pour JavaScript. Tous les environnements d' Node.js exécution Lambda pris en charge incluent le SDK pour la version 3. JavaScript

Toutefois, nous vous recommandons vivement d'inclure les clients AWS SDK dont vous avez besoin dans votre package de déploiement. Cela permet d'optimiser la rétrocompatibilité lors des futures mises à jour de l'environnement d'exécution Lambda. Ne vous fiez au SDK fourni par l'environnement d'exécution que lorsque vous ne pouvez pas inclure de packages supplémentaires (par exemple, lorsque vous utilisez l'éditeur de code de la console Lambda ou du code en ligne dans un modèle). AWS CloudFormation

Pour ajouter des dépendances au SDK à votre fonction, utilisez la commande `npm install` correspondant aux clients SDK spécifiques dont vous avez besoin. Dans l'exemple de code, nous avons utilisé le client Amazon S3. Ajoutez cette dépendance en exécutant la commande suivante dans le répertoire qui contient votre fichier `package.json` :

```
npm install @aws-sdk/client-s3
```

Dans le code de fonction, importez le client et les commandes dont vous avez besoin, comme le montre l'exemple de fonction :

```
import { S3Client, PutObjectCommand } from '@aws-sdk/client-s3';
```

Initialisez ensuite un client Amazon S3 :

```
const s3Client = new S3Client();
```

Dans cet exemple, nous avons initialisé notre client Amazon S3 en dehors de la fonction de gestionnaire principale pour éviter d'avoir à l'initialiser à chaque fois que nous invoquons notre fonction. Après avoir initialisé votre client SDK, vous pouvez l'utiliser pour effectuer des appels d'API pour ce AWS service. L'exemple de code appelle l'action d'PutObjectAPI Amazon S3 comme suit :

```
const command = new PutObjectCommand({
    Bucket: bucketName,
    Key: key,
    Body: receiptContent
});
```

Accès aux variables d'environnement

Dans le code de votre gestionnaire, vous pouvez référencer n'importe quelle variable d'environnement à l'aide de `process.env`. Dans cet exemple, nous référençons la variable d'environnement `RECEIPT_BUCKET` définie à l'aide des lignes de code suivantes :

```
// Access environment variables
const bucketName = process.env.RECEIPT_BUCKET;
if (!bucketName) {
    throw new Error('RECEIPT_BUCKET environment variable is not set');
}
```

Utilisation de l'état global

Lambda exécute votre code statique pendant la phase d'initialisation avant d'invoquer votre fonction pour la première fois. Les ressources créées pendant l'initialisation restent en mémoire entre les invocations, ce qui vous évite d'avoir à les créer chaque fois que vous invoquez votre fonction.

Dans l'exemple de code, le code d'initialisation du client S3 se trouve en dehors du gestionnaire. L'exécution initialise le client avant que la fonction n'exécute son premier événement, et le client reste disponible pour être réutilisé pendant toutes les invocations.

Meilleures pratiques en matière de code pour les Node.js fonctions d'événement Lambda

Suivez ces instructions pour créer des fonctions Lambda :

- Séparez le gestionnaire Lambda de votre logique principale. Cela vous permet de créer une fonction testable plus unitaire.
- Contrôlez les dépendances du package de déploiement de vos fonctions. L'environnement AWS Lambda d'exécution contient un certain nombre de bibliothèques. Pour les Node.js environnements d'exécution et Python, ceux-ci incluent les AWS SDK. Pour activer le dernier ensemble de mises à jour des fonctionnalités et de la sécurité, Lambda met régulièrement à jour ces bibliothèques. Ces mises à jour peuvent introduire de subtiles modifications dans le comportement de votre fonction Lambda. Pour disposer du contrôle total des dépendances que votre fonction utilise, empaquetez toutes vos dépendances avec votre package de déploiement.
- Réduisez la complexité de vos dépendances. Privilégiez les infrastructures plus simples qui se chargent rapidement au démarrage de l'environnement d'exécution.

- Réduisez la taille de votre package de déploiement selon ses besoins d'exécution. Cela contribue à réduire le temps nécessaire au téléchargement et à la décompression de votre package de déploiement avant l'invocation.

Tirez parti de la réutilisation de l'environnement d'exécution pour améliorer les performances de votre fonction. Initialisez les clients SDK et les connexions à la base de données en dehors du gestionnaire de fonctions et mettez en cache les actifs statiques localement dans le répertoire `/tmp`. Les invocations ultérieures traitées par la même instance de votre fonction peuvent réutiliser ces ressources. Cela permet d'économiser des coûts, tout en réduisant le temps d'exécution de la fonction.

Pour éviter des éventuelles fuites de données entre les invocations, n'utilisez pas l'environnement d'exécution pour stocker des données utilisateur, des événements ou d'autres informations ayant un impact sur la sécurité. Si votre fonction repose sur un état réversible qui ne peut pas être stocké en mémoire dans le gestionnaire, envisagez de créer une fonction distincte ou des versions distinctes d'une fonction pour chaque utilisateur.

Utilisez une directive keep-alive pour maintenir les connexions persistantes. Lambda purge les connexions inactives au fil du temps. Si vous tentez de réutiliser une connexion inactive lorsque vous invoquez une fonction, cela entraîne une erreur de connexion. Pour maintenir votre connexion persistante, utilisez la directive Keep-alive associée à votre environnement d'exécution. Pour un exemple, voir Réutilisation des connexions avec Keep-Alive in Node.js.

Utilisez des variables d'environnement pour transmettre des paramètres opérationnels à votre fonction. Par exemple, si vous écrivez dans un compartiment Amazon S3 au lieu de coder en dur le nom du compartiment dans lequel vous écrivez, configurez le nom du compartiment comme variable d'environnement.

Évitez d'utiliser des invocations récursives dans votre fonction Lambda, lorsque la fonction s'invoque elle-même ou démarre un processus susceptible de l'invoquer à nouveau. Cela peut entraîner un volume involontaire d'invocations de fonction et des coûts accrus. Si vous constatez un volume involontaire d'invocations, définissez immédiatement la simultanéité réservée à la fonction sur `0` afin de limiter toutes les invocations de la fonction, pendant que vous mettez à jour le code.

N'utilisez pas d'API non publiques non documentées dans le code de votre fonction Lambda. Pour les AWS Lambda environnements d'exécution gérés, Lambda applique régulièrement des mises à jour fonctionnelles et de sécurité aux API internes de Lambda. Ces mises à jour internes de l'API peuvent être incompatibles avec les versions antérieures, entraînant des conséquences imprévues telles que

des échecs d'invocation si votre fonction dépend de ces API non publiques. Consultez la Référence d'API pour obtenir la liste des API accessibles au public.

Écriture du code idempotent. L'écriture de code idempotent pour vos fonctions garantit ne gestion identique des événements dupliqués. Votre code doit valider correctement les événements et gérer correctement les événements dupliqués. Pour de plus amples informations, veuillez consulterComment faire en sorte que ma fonction Lambda soit idempotente ?.

Déployez les fonctions d'événement Node.js Lambda avec des archives de fichiers .zip

Le code de votre AWS Lambda fonction comprend un fichier .js ou .mjs contenant le code du gestionnaire de votre fonction, ainsi que les packages et modules supplémentaires dont dépend votre code. Pour déployer ce code de fonction vers Lambda, vous utilisez un package de déploiement. Ce package peut être une archive de fichier .zip ou une image de conteneur. Pour plus d'informations sur l'utilisation d'images de conteneur avec Node.js, voir Déployer des fonctions d'événement Node.js Lambda avec des images de conteneur.

Pour créer votre package de déploiement sous forme d'archive de fichier .zip, vous pouvez utiliser l'utilitaire d'archivage .zip intégré à votre outil de ligne de commande, ou tout autre utilitaire .zip tel que 7zip. Les exemples présentés dans les sections suivantes supposent que vous utilisez un outil `zip` de ligne de commande dans un environnement Linux ou macOS. Pour utiliser les mêmes commandes sous Windows, vous pouvez installer le sous-système Windows pour Linux afin d'obtenir une Windows-integrated version d'Ubuntu et de Bash.

Notez que Lambda utilise les autorisations de fichiers POSIX. Ainsi, vous pourriez devoir définir des autorisations pour le dossier du package de déploiement avant de créer l'archive de fichiers .zip.

Rubriques

- Dépendances d'exécution dans Node.js
- Création d'un package de déploiement .zip sans dépendances
- Création d'un package de déploiement .zip avec dépendances
- Création d'une Node.js couche pour vos dépendances
- Chemin de recherche des dépendances et bibliothèques incluses dans l'exécution
- Création et mise à jour des fonctions d'événement Node.js Lambda à l'aide de fichiers .zip

Dépendances d'exécution dans Node.js

Pour les fonctions d'événement Lambda qui utilisent le Node.js runtime, une dépendance peut être n'importe quel Node.js module. Le Node.js moteur d'exécution inclut un certain nombre de bibliothèques courantes, ainsi qu'une version du AWS SDK pour JavaScript. Tous les environnements d' Node.js exécution pris en charge incluent la version 3 du SDK. Pour utiliser la version 2 du SDK, vous devez ajouter le SDK à votre package de déploiement de fichiers .zip. Pour savoir quelle version spécifique du kit SDK est incluse dans l'environnement d'exécution que vous utilisez, consultez the section called "Runtime-included Versions du SDK".

Lambda met régulièrement à jour les bibliothèques du SDK dans l' Node.js environnement d'exécution pour inclure les dernières fonctionnalités et mises à niveau de sécurité. Lambda applique également des correctifs de sécurité et des mises à jour aux autres bibliothèques incluses dans l'exécution. Pour avoir un contrôle total sur les dépendances de votre package, vous pouvez ajouter votre version préférée de n'importe quelle dépendance incluse dans l'exécution à votre package de déploiement. Par exemple, si vous souhaitez utiliser une version particulière du SDK pour JavaScript, vous pouvez l'inclure dans votre fichier .zip en tant que dépendance. Pour plus d'informations sur l'ajout de dépendances incluses dans l'exécution à votre fichier .zip, consultez Chemin de recherche des dépendances et bibliothèques incluses dans l'exécution.

Dans le cadre du modèle de responsabilité partagée AWS, vous êtes responsable de la gestion de toutes les dépendances dans les packages de déploiement de vos fonctions. Cela inclut l'application de mises à jour et de correctifs de sécurité. Pour mettre à jour les dépendances dans le package de déploiement de votre fonction, créez d'abord un nouveau fichier .zip, puis chargez-le sur Lambda. Pour plus d'informations, consultez Création d'un package de déploiement .zip avec dépendances et Création et mise à jour des fonctions d'événement Node.js Lambda à l'aide de fichiers .zip.

Création d'un package de déploiement .zip sans dépendances

Si le code de votre fonction ne comporte aucune dépendance, à l'exception des bibliothèques incluses dans le runtime Lambda, votre fichier .zip contient uniquement le `index.mjs` fichier `index.js` ou contenant le code du gestionnaire de votre fonction. Utilisez votre utilitaire zip préféré pour créer un fichier .zip avec votre fichier `index.js` ou `index.mjs` à la racine. Si le fichier contenant le code de votre gestionnaire ne se trouve pas à la racine de votre fichier .zip, Lambda ne pourra pas exécuter votre code.

Pour savoir comment déployer votre fichier .zip pour créer une nouvelle fonction Lambda ou mettre à jour une fonction Lambda existante, veuillez consulter la rubrique Création et mise à jour des fonctions d'événement Node.js Lambda à l'aide de fichiers .zip.

Création d'un package de déploiement .zip avec dépendances

Si le code de votre fonction dépend de packages ou de modules qui ne sont pas inclus dans le Node.js runtime Lambda, vous pouvez soit ajouter ces dépendances à votre fichier .zip avec votre code de fonction, soit utiliser une couche Lambda. Les instructions de cette section vous indiquent comment inclure vos dépendances dans votre package de déploiement .zip. Pour obtenir des instructions sur la façon d'inclure vos dépendances dans une couche, voir the section called "Création d'une Node.js couche pour vos dépendances".

L'exemple de commandes de CLI suivant crée un fichier .zip nommé `my_deployment_package.zip` contenant le fichier `index.js` ou `index.mjs` avec le gestionnaire de code de votre fonction et ses dépendances. Dans l'exemple, vous installez les dépendances à l'aide du gestionnaire de packages npm.

Pour créer le package de déploiement

1. Accédez au répertoire du projet qui contient votre fichier de code source `index.js` ou `index.mjs`. Dans cet exemple, le répertoire est nommé `my_function`.

   ```
   cd my_function
   ```

2. Installez les bibliothèques requises pour votre fonction dans le répertoire `node_modules` à l'aide de la commande `npm install`. Dans cet exemple, vous installez Kit SDK AWS X-Ray pour Node.js.

   ```
   npm install aws-xray-sdk
   ```

   Cela crée une structure de dossiers similaire à ce qui suit :

   ```
   ~/my_function
   ### index.mjs
   ### node_modules
       ### async
       ### async-listener
       ### atomic-batcher
       ### aws-sdk
       ### aws-xray-sdk
       ### aws-xray-sdk-core
   ```

   Vous pouvez également ajouter des modules personnalisés que vous créez vous-même à votre package de déploiement. Créez un répertoire sous `node_modules` portant le nom de votre module et enregistrez-y vos packages écrits personnalisés.

3. Créez un fichier .zip reprenant le contenu de votre dossier de projet à la racine. Utilisez l'option `r` (récursive) pour veiller à ce que zip compresse les sous-dossiers.

   ```
   zip -r my_deployment_package.zip .
   ```

Création d'une Node.js couche pour vos dépendances

Les instructions de cette section vous indiquent comment inclure les dépendances dans une couche. Pour obtenir des instructions sur la façon d'inclure vos dépendances dans votre package de déploiement, voir the section called "Création d'un package de déploiement .zip avec dépendances". Pour plus d'informations sur la création et la gestion des Node.js couches, consultezthe section called "Layers".

Lorsque vous ajoutez une couche à une fonction, Lambda charge le contenu de la couche dans le répertoire `/opt` de cet environnement d'exécution. Pour chaque exécution Lambda, la variable `PATH` inclut déjà des chemins de dossiers spécifiques dans le répertoire `/opt`. Pour garantir que Lambda capture le contenu de votre couche, le fichier .zip de votre couche doit avoir ses dépendances un des chemins de dossier suivants :

- `nodejs/node_modules`
- `nodejs/node18/node_modules (NODE_PATH)`
- `nodejs/node20/node_modules (NODE_PATH)`
- `nodejs/node22/node_modules (NODE_PATH)`

Par exemple, la structure du fichier .zip de votre couche peut ressembler à ce qui suit :

```
xray-sdk.zip
# nodejs/node_modules/aws-xray-sdk
```

En outre, Lambda détecte automatiquement toutes les bibliothèques dans le répertoire `/opt/lib` et tous les fichiers binaires dans le répertoire `/opt/bin`. Pour que Lambda trouve correctement le contenu de votre couche, vous pouvez aussi créer une couche avec la structure suivante :

```
custom-layer.zip
# lib
    | lib_1
    | lib_2
# bin
    | bin_1
    | bin_2
```

Après avoir empaqueté votre couche, reportez-vous à the section called "Création et suppression de couches" et à the section called "Ajout de couches" pour terminer la configuration de votre couche.

Chemin de recherche des dépendances et bibliothèques incluses dans l'exécution

Le Node.js moteur d'exécution inclut un certain nombre de bibliothèques courantes, ainsi qu'une version du AWS SDK pour JavaScript. Si vous souhaitez utiliser une version différente d'une bibliothèque incluse dans l'exécution, vous pouvez le faire en l'associant à votre fonction ou en l'ajoutant en tant que dépendance dans votre package de déploiement. Par exemple, vous pouvez utiliser une version différente du kit SDK en l'ajoutant à votre package de déploiement .zip. Vous pouvez également l'inclure dans une couche Lambda pour votre fonction.

Lorsque vous utilisez une `require` instruction `import` or dans votre code, le Node.js moteur d'exécution recherche les répertoires du `NODE_PATH` chemin jusqu'à ce qu'il trouve le module. Par défaut, le premier emplacement dans lequel recherche l'exécution est le répertoire dans lequel votre package de déploiement .zip est décompressé et monté (`/var/task`). Si vous incluez une version d'une bibliothèque incluse dans l'environnement d'exécution dans votre package de déploiement, cette version a priorité sur la version incluse dans le moteur d'exécution. Les dépendances de votre package de déploiement ont également la priorité sur les dépendances des couches.

Lorsque vous ajoutez une dépendance à une couche, Lambda l'extrait vers `/opt/nodejs/nodexx/node_modules`, où `nodexx` représente la version de l'exécution que vous utilisez. Dans le chemin de recherche, ce répertoire a la priorité sur le répertoire contenant les bibliothèques incluses dans l'exécution (`/var/lang/lib/node_modules`). Les bibliothèques des couches de fonctions ont donc la priorité sur les versions incluses dans l'exécution.

Vous pouvez voir le chemin de recherche complet de votre fonction Lambda en ajoutant la ligne de code suivante.

```
console.log(process.env.NODE_PATH)
```

Vous pouvez également ajouter des dépendances dans un dossier distinct au sein de votre package .zip. Par exemple, vous pouvez ajouter un module personnalisé à un dossier votre package .zip appelé `common`. Lorsque votre package .zip est décompressé et monté, ce dossier est placé dans le répertoire `/var/task`. Pour utiliser une dépendance provenant d'un dossier de votre package de déploiement .zip dans votre code, utilisez une instruction `import { } from` ou `const { } = require()`, selon que vous utilisez la résolution du module CJS ou ESM. Par exemple :

```
import { myModule } from './common'
```

Si vous regroupez votre code à `esbuild`, `rollup`, ou similaire, les dépendances utilisées par votre fonction sont regroupées dans un ou plusieurs fichiers. Nous vous recommandons d'utiliser cette

méthode pour vendre des dépendances chaque fois que cela est possible. Par rapport à l'ajout de dépendances à votre package de déploiement, le regroupement de votre code améliore les performances grâce à la réduction I/O des opérations.

Création et mise à jour des fonctions d'événement Node.js Lambda à l'aide de fichiers .zip

Une fois que vous avez créé votre package de déploiement .zip, vous pouvez l'utiliser pour créer une nouvelle fonction Lambda ou mettre à jour une fonction Lambda existante. Vous pouvez déployer votre package .zip à l'aide de la console Lambda, de l'API Lambda et AWS Command Line Interface de l'API Lambda. Vous pouvez également créer et mettre à jour des fonctions Lambda à l'aide de l' AWS Serverless Application Model (AWS SAM) et de CloudFormation.

La taille maximale d'un package de déploiement .zip pour Lambda est de 250 Mo (décompressé). Notez que cette limite s'applique à la taille combinée de tous les fichiers que vous chargez, y compris les couches Lambda.

Le runtime Lambda a besoin d'une autorisation pour lire les fichiers de votre package de déploiement. Dans la notation octale des autorisations Linux, Lambda a besoin de 644 autorisations pour les fichiers non exécutables (rw-r--r--) et de 755 autorisations (rwxr-xr-x) pour les répertoires et les fichiers exécutables.

Sous Linux et macOS, utilisez la commande `chmod` pour modifier les autorisations de fichiers sur les fichiers et les répertoires de votre package de déploiement. Par exemple, pour octroyer à un fichier non exécutable les autorisations correctes, exécutez la commande suivante.

```
chmod 644 <filepath>
```

Pour modifier les autorisations relatives aux fichiers dans Windows, voir Définir, afficher, modifier ou supprimer des autorisations sur un objet dans la documentation Microsoft Windows.

> **Note**
>
> Si vous n'octroyez pas à Lambda les autorisations dont il a besoin pour accéder aux répertoires de votre package de déploiement, Lambda définit les autorisations de ces répertoires à 755 (rwxr-xr-x).

Création et mise à jour de fonctions avec des fichiers .zip à l'aide de la console

Pour créer une nouvelle fonction, vous devez d'abord créer la fonction dans la console, puis charger votre archive .zip. Pour mettre à jour une fonction existante, ouvrez la page de votre fonction, puis suivez la même procédure pour ajouter votre fichier .zip mis à jour.

Si votre fichier .zip fait moins de 50 Mo, vous pouvez créer ou mettre à jour une fonction en chargeant le fichier directement à partir de votre ordinateur local. Pour les fichiers .zip de plus de 50 Mo, vous devez d'abord charger votre package dans un compartiment Amazon S3. Pour savoir comment charger un fichier dans un compartiment Amazon S3 à l'aide du Console de gestion AWS, consultez Getting started with Amazon S3. Pour télécharger des fichiers à l'aide de AWS CLI, voir Déplacer des objets dans le guide de AWS CLI l'utilisateur.

> **Note**
>
> Vous ne pouvez pas modifier le type de package de déploiement (.zip ou image de conteneur) d'une fonction existante. Par exemple, vous ne pouvez pas convertir une fonction d'image de conteneur pour utiliser un fichier d'archive .zip à la place. Vous devez créer une nouvelle fonction.

Pour créer une nouvelle fonction (console)

1. Ouvrez la page Event Functions de la console Lambda et choisissez Create Event Function.
2. Choisissez Créer à partir de zéro.
3. Sous Informations de base, procédez comme suit :
   a. Pour Nom de la fonction, saisissez le nom de la fonction.
   b. Pour Exécution, sélectionnez l'exécution que vous souhaitez utiliser.
   c. (Facultatif) Pour Architecture, choisissez l'architecture de l'ensemble des instructions pour votre fonction. L'architecture par défaut est x86_64. Assurez-vous que le package de déploiement .zip pour votre fonction est compatible avec l'architecture de l'ensemble d'instructions que vous sélectionnez.
4. (Facultatif) Sous Permissions (Autorisations), développez Change default execution role (Modifier le rôle d'exécution par défaut). Vous pouvez créer un rôle d'exécution ou en utiliser un existant.

5. Choisissez Create Event Function. Lambda crée une fonction de base « Hello world » à l'aide de l'exécution de votre choix.

Pour charger une archive .zip à partir de votre ordinateur local (console)

1. Sur la page Event Functions de la console Lambda, choisissez la fonction pour laquelle vous souhaitez télécharger le fichier .zip.
2. Sélectionnez l'onglet Code.
3. Dans le volet Source du code, choisissez Charger à partir de.
4. Choisissez Fichier .zip.
5. Pour charger un fichier .zip, procédez comme suit :
   a. Sélectionnez Charger, puis choisissez votre fichier .zip dans le sélecteur de fichiers.
   b. Choisissez Ouvrir.
   c. Cliquez sur Enregistrer.

Pour charger une archive .zip depuis un compartiment Amazon S3 (console)

1. Sur la page Event Functions de la console Lambda, choisissez la fonction pour laquelle vous souhaitez télécharger un nouveau fichier .zip.
2. Sélectionnez l'onglet Code.
3. Dans le volet Source du code, choisissez Charger à partir de.
4. Choisissez l'emplacement Amazon S3.
5. Collez l'URL du lien Amazon S3 de votre fichier .zip et choisissez Enregistrer.

Mise à jour des fonctions du fichier .zip à l'aide de l'éditeur de code de la console

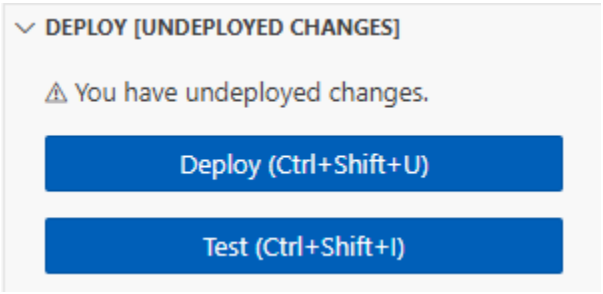
Pour certaines fonctions avec des packages de déploiement .zip, vous pouvez utiliser l'éditeur de code intégré de la console Lambda pour mettre à jour le code de votre fonction directement. Pour utiliser cette fonctionnalité, votre fonction doit répondre aux critères suivants :

- Votre fonction doit utiliser l'un des environnements d'exécution du langage interprété (Python ou Ruby) Node.js
- La taille du package de déploiement de votre fonction doit être inférieure à 50 Mo (décompressé).

Le code des fonctions avec les packages de déploiement d'images de conteneurs ne peut pas être édité directement dans la console.

Pour mettre à jour le code de fonction à l'aide de l'éditeur de code de la console

1. Ouvrez la page Event Functions de la console Lambda et sélectionnez votre fonction.
2. Sélectionnez l'onglet Code.
3. Dans le volet Source du code, sélectionnez votre fichier de code source et modifiez-le dans l'éditeur de code intégré.
4. Dans la section DÉPLOYER, choisissez Déployer pour mettre à jour le code de votre fonction :



Création et mise à jour de fonctions avec des fichiers .zip à l'aide du AWS CLI

Vous pouvez utiliser l'AWS CLI pour créer une nouvelle fonction ou pour mettre à jour une fonction existante à l'aide d'un fichier .zip. Utilisez les commandes create-function et update-function-code pour déployer votre package .zip. Si votre fichier .zip est inférieur à 50 Mo, vous pouvez charger le package .zip à partir d'un emplacement de fichier sur votre machine de génération locale. Pour les fichiers plus volumineux, vous devez charger votre package .zip à partir d'un compartiment Amazon S3. Pour savoir comment charger un fichier dans un compartiment Amazon S3 à l'aide du AWS CLI, consultez la section Déplacer des objets dans le guide de AWS CLI l'utilisateur.

> **Note**
>
> Si vous chargez votre fichier .zip depuis un compartiment Amazon S3 à l'aide de AWS CLI, le compartiment doit se trouver au même endroit Région AWS que votre fonction.

Pour créer une nouvelle fonction à l'aide d'un fichier .zip avec le AWS CLI, vous devez spécifier les éléments suivants :

- Le nom de votre fonction (`--function-name`)

- L'exécution de votre fonction (`--runtime`)
- L'Amazon Resource Name (ARN) du rôle d'exécution de votre fonction (`--role`)
- Le nom de la méthode du gestionnaire dans votre code de fonction (`--handler`)

Vous devez également indiquer l'emplacement de votre fichier .zip. Si votre fichier .zip se trouve dans un dossier sur votre machine de génération locale, utilisez l'option `--zip-file` pour spécifier le chemin d'accès du fichier, comme le montre l'exemple de commande suivant.

```
aws lambda create-function --function-name myFunction \
--runtime nodejs24.x --handler index.handler \
--role arn:aws:iam::111122223333:role/service-role/my-lambda-role \
--zip-file fileb://myFunction.zip
```

Pour spécifier l'emplacement du fichier .zip dans un compartiment Amazon S3, utilisez l'option `--code` comme le montre l'exemple de commande suivant. Vous devez uniquement utiliser le paramètre `S3ObjectVersion` pour les objets soumis à la gestion des versions.

```
aws lambda create-function --function-name myFunction \
--runtime nodejs24.x --handler index.handler \
--role arn:aws:iam::111122223333:role/service-role/my-lambda-role \
--code S3Bucket=amzn-s3-demo-
bucket,S3Key=myFileName.zip,S3ObjectVersion=myObjectVersion
```

Pour mettre à jour une fonction existante à l'aide de l'interface de ligne de commande, vous devez spécifier le nom de votre fonction à l'aide du paramètre `--function-name`. Vous devez également spécifier l'emplacement du fichier .zip que vous souhaitez utiliser pour mettre à jour votre code de fonction. Si votre fichier .zip se trouve dans un dossier sur votre machine de génération locale, utilisez l'option `--zip-file` pour spécifier le chemin d'accès du fichier, comme le montre l'exemple de commande suivant.

```
aws lambda update-function-code --function-name myFunction \
--zip-file fileb://myFunction.zip
```

Pour spécifier l'emplacement du fichier .zip dans un compartiment Amazon S3, utilisez les options `--s3-bucket` et `--s3-key` comme le montre l'exemple de commande suivant. Vous devez uniquement utiliser le paramètre `--s3-object-version` pour les objets soumis à la gestion des versions.

```
aws lambda update-function-code --function-name myFunction \
--s3-bucket amzn-s3-demo-bucket --s3-key myFileName.zip --s3-object-version myObject
 Version
```

Création et mise à jour de fonctions avec des fichiers .zip à l'aide de l'API Lambda

Pour créer et mettre à jour des fonctions à l'aide d'une archive de fichiers .zip, utilisez les opérations d'API suivantes :

- CreateFunction
- UpdateFunctionCode

Création et mise à jour de fonctions avec des fichiers .zip à l'aide de AWS SAM

The AWS Serverless Application Model (AWS SAM) est une boîte à outils qui permet de rationaliser le processus de création et d'exécution d'applications sans serveur sur AWS. Vous définissez les ressources de votre application dans un modèle YAML ou JSON et vous utilisez l'interface de ligne de AWS SAM commande (AWS SAM CLI) pour créer, empaqueter et déployer vos applications. Lorsque vous créez une fonction Lambda à partir d'un AWS SAM modèle, elle crée AWS SAM automatiquement un package de déploiement ou une image de conteneur .zip avec le code de votre fonction et les dépendances que vous spécifiez. Pour en savoir plus sur l'utilisation des fonctions Lambda AWS SAM pour créer et déployer des fonctions Lambda, consultez Getting started with AWS SAM dans le Guide du AWS Serverless Application Model développeur.

Vous pouvez également l'utiliser AWS SAM pour créer une fonction Lambda à l'aide d'une archive de fichiers .zip existante. Pour créer une fonction Lambda à l'aide de AWS SAM, vous pouvez enregistrer votre fichier .zip dans un compartiment Amazon S3 ou dans un dossier local sur votre machine de génération. Pour savoir comment charger un fichier dans un compartiment Amazon S3 à l'aide du AWS CLI, consultez la section Déplacer des objets dans le guide de AWS CLI l'utilisateur.

Dans votre AWS SAM modèle, la `AWS::Serverless::Function` ressource spécifie votre fonction Lambda. Dans cette ressource, définissez les propriétés suivantes pour créer une fonction à l'aide d'une archive de fichiers .zip :

- `PackageType` : défini sur `Zip`
- `CodeUri`- défini sur l'URI Amazon S3, le chemin d'accès au dossier local ou à l'FunctionCodeobjet du code de fonction
- `Runtime` : défini sur votre exécution choisie

Ainsi AWS SAM, si votre fichier .zip est supérieur à 50 Mo, vous n'avez pas besoin de le télécharger au préalable dans un compartiment Amazon S3. AWS SAM peut télécharger des packages .zip jusqu'à la taille maximale autorisée de 250 Mo (décompressés) à partir d'un emplacement sur votre machine de compilation locale.

Pour en savoir plus sur le déploiement de fonctions à l'aide d'un fichier .zip dans AWS SAM, voir AWS::Serverless::Function dans le manuel du AWS SAM développeur.

Création et mise à jour de fonctions avec des fichiers .zip à l'aide de CloudFormation

Vous pouvez l'utiliser CloudFormation pour créer une fonction Lambda à l'aide d'une archive de fichiers .zip. Pour créer une fonction Lambda à partir d'un fichier .zip, vous devez d'abord charger votre fichier dans un compartiment Amazon S3. Pour savoir comment charger un fichier dans un compartiment Amazon S3 à l'aide du AWS CLI, consultez la section Déplacer des objets dans le guide de AWS CLI l'utilisateur.

Dans votre CloudFormation modèle, la `AWS::Lambda::Function` ressource spécifie votre fonction Lambda. Dans cette ressource, définissez les propriétés suivantes pour créer une fonction à l'aide d'une archive de fichiers .zip :

- `PackageType` : défini sur `Zip`
- `Code` : saisissez le nom du compartiment Amazon S3 et le nom du fichier .zip dans les champs `S3Bucket` et `S3Key`
- `Runtime` : défini sur votre exécution choisie

Le fichier .zip CloudFormation généré ne peut pas dépasser 4 Mo. Pour en savoir plus sur le déploiement de fonctions à l'aide d'un fichier .zip dans CloudFormation, voir AWS::Lambda::Function dans le guide de l'CloudFormation utilisateur.

Déployer des fonctions d'événement Node.js Lambda avec des images de conteneur

Il existe trois méthodes pour créer une image de conteneur pour une fonction d'événement Node.js Lambda :

- À l'aide d'un AWS image de base pour Node.js

  Les images de base AWS sont préchargées avec une exécution du langage, un client d'interface d'exécution pour gérer l'interaction entre Lambda et votre code de fonction, et un émulateur d'interface d'exécution pour les tests locaux.
- À l'aide d'un AWS OS-only image de base

  AWS OS-only les images de base contiennent une distribution Amazon Linux et l'émulateur d'interface d'exécution. Ces images sont couramment utilisées pour créer des images de conteneur pour les langages compilés, tels que Go et Rust, et pour une langue ou une version linguistique pour laquelle Lambda ne fournit pas d'image de base, telle que Node.js 19. Vous pouvez également utiliser des images OS-only de base pour implémenter un environnement d'exécution personnalisé. Pour rendre l'image compatible avec Lambda, vous devez inclure le client d'interface d'exécution pour Node.js dans l'image.
- Utilisation d'une image non AWS basique

  Vous pouvez utiliser une autre image de base à partir d'un autre registre de conteneur, comme Alpine Linux ou Debian. Vous pouvez également utiliser une image personnalisée créée par votre organisation. Pour rendre l'image compatible avec Lambda, vous devez inclure le client d'interface d'exécution pour Node.js dans l'image.

> **Tip**
>
> Pour réduire le temps nécessaire à l'activation des fonctions du conteneur Lambda, consultez Utiliser des générations en plusieurs étapes (français non garanti) dans la documentation Docker. Pour créer des images de conteneur efficaces, suivez la section Bonnes pratiques pour l'écriture de Dockerfiles (français non garanti).

Cette page explique comment créer, tester et déployer des images de conteneur pour Lambda.

Rubriques

- AWS images de base pour Node.js

- À l'aide d'un AWS image de base pour Node.js
- Utilisation d'une autre image de base avec le client d'interface d'exécution

AWS images de base pour Node.js

AWS fournit les images de base suivantes pour Node.js :

Étiquettes	Environnement d'exécution	Système d'exploitation	Dockerfile	Obsolescence
26	Node.js 26	Amazon Linux	Dockerfile pour 26 ans Node.js GitHub	Non planifié
24	Node.js 24	Amazon Linux	Dockerfile pour 24 ans Node.js GitHub	30 avril 2028
22	Node.js 22	Amazon Linux	Dockerfile pour 22 ans Node.js GitHub	30 avril 2027

Référentiel Amazon ECR : gallery.ecr. aws/lambda/nodejs

Les Node.js 20 images de base et suivantes sont basées sur l'image de conteneur minimale Amazon Linux 2023. Les images de base antérieures utilisaient Amazon Linux 2. AL2023 offre plusieurs avantages par rapport à Amazon Linux2, notamment un encombrement de déploiement réduit et des versions mises à jour de bibliothèques telles que `glibc`.

AL2023-based les images utilisent `microdnf` (lié par un lien symboliquednf) comme gestionnaire de packages au lieu deyum, qui est le gestionnaire de packages par défaut dans Amazon Linux 2. `microdnf`est une implémentation autonome de. `dnf` Pour obtenir la liste des packages inclus dans les AL2023-based images, reportez-vous aux colonnes Conteneur minimal de la section Comparaison des packages installés sur Amazon Linux 2023 Container Images. Pour plus d'informations sur les différences entre AL2023 et Amazon Linux 2, consultez Introducing the Amazon Linux 2023 runtime for AWS Lambda sur le blog AWS Compute.

> **Note**
>
> Pour exécuter AL2023-based des images localement, y compris avec AWS Serverless Application Model (AWS SAM), vous devez utiliser Docker version 20.10.10 ou ultérieure.

À l'aide d'un AWS image de base pour Node.js

Conditions préalables

Pour exécuter la procédure indiquée dans cette section, vous devez satisfaire aux exigences suivantes :

- AWS CLI version 2
- Docker (version minimale 25.0.0)
- Le plug-in buildx Docker.
- Node.js

Création d'une image à partir d'une image de base

Pour créer une image de conteneur à partir d'un AWS image de base pour Node.js

1. Créez un répertoire pour le projet, puis passez à ce répertoire.

   ```
   mkdir example
   cd example
   ```

2. Créez un nouveau Node.js projet avec`npm`. Appuyez sur `Enter` pour accepter les options par défaut fournies dans l'expérience interactive.

   ```
   npm init
   ```

3. Créez un nouveau fichier appelé `index.js`. Vous pouvez ajouter l'exemple de code de fonction suivant au fichier pour le tester, ou utiliser le vôtre.

   Example Gestionnaire CommonJS

   ```
   exports.handler = async (event) => {
       const response = {
   ```

```
        statusCode: 200,
        body: JSON.stringify('Hello from Lambda!'),
    };
    return response;
};
```

4. Si votre fonction dépend de bibliothèques autres que celles-ci AWS SDK pour JavaScript, utilisez npm pour les ajouter à votre package.
5. Créez un nouveau Dockerfile avec la configuration suivante :

   - Définir la propriété FROM sur l'URI de l'image de base.
   - Utilisez la commande COPY pour copier le code de fonction et les dépendances d'{LAMBDA_TASK_ROOT}exécution dans une variable d'Lambda-defined environnement.
   - Définir l'argument CMD pour le gestionnaire de la fonction Lambda.

   Notez que l'exemple de Dockerfile n'inclut pas d'instruction USER. Lorsque vous déployez une image de conteneur sur Lambda, Lambda définit automatiquement un utilisateur Linux par défaut disposant d'autorisations de moindre privilège. Ceci est différent du comportement standard de Docker qui est défini par défaut par l'utilisateur `root` lorsqu'aucune instruction USER n'est fournie.

   Example Dockerfile

```
FROM public.ecr.aws/lambda/nodejs:22

# Copy function code
COPY index.js ${LAMBDA_TASK_ROOT}

# Set the CMD to your handler (could also be done as a parameter override outside
 of the Dockerfile)
CMD [ "index.handler" ]
```

6. Générez l'image Docker à l'aide de la commande docker build. L'exemple suivant nomme l'image `docker-image` et lui donne la balise `test`. Pour rendre votre image compatible avec Lambda, vous devez utiliser l'option `--provenance=false`.

```
docker buildx build --platform linux/amd64 --provenance=false -t docker-image:test
 .
```

> **Note**
>
> La commande spécifie l'option `--platform linux/amd64` pour garantir la compatibilité de votre conteneur avec l'environnement d'exécution Lambda, quelle que soit l'architecture de votre machine de génération. Si vous avez l'intention de créer une fonction Lambda à l'aide de l'architecture du jeu d'instructions ARM64, veillez à modifier la commande pour utiliser plutôt l'option `--platform linux/arm64`.

(Facultatif) Testez l'image localement

1. Démarrez votre image Docker à l'aide de la commande docker run. Dans cet exemple, `docker-image` est le nom de l'image et `test` est la balise.

   ```
   docker run --platform linux/amd64 -p 9000:8080 docker-image:test
   ```

   Cette commande exécute l'image en tant que conteneur et crée un point de terminaison local à `localhost:9000/2015-03-31/functions/function/invocations`.

   > **Note**
   >
   > Si vous avez créé l'image Docker pour l'architecture du jeu d'instructions ARM64, veillez à utiliser l'option `--platform linux/arm64` plutôt que `--platform linux/amd64`.

2. À partir d'une nouvelle fenêtre de terminal, publiez un événement au point de terminaison local.

   Linux/macOS

   Sous Linux et macOS, exécutez la commande `curl` suivante :

   ```
   curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d '{}'
   ```

   Cette commande invoque la fonction avec un événement vide et renvoie une réponse. Si vous utilisez votre propre code de fonction plutôt que l'exemple de code de fonction, vous pouvez invoquer la fonction avec une charge utile JSON. Exemple :

```
curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d
 '{"payload":"hello world!"}'
```

PowerShell

Dans PowerShell, exécutez la `Invoke-WebRequest` commande suivante :

```
Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/
invocations" -Method Post -Body '{}' -ContentType "application/json"
```

Cette commande invoque la fonction avec un événement vide et renvoie une réponse. Si vous utilisez votre propre code de fonction plutôt que l'exemple de code de fonction, vous pouvez invoquer la fonction avec une charge utile JSON. Exemple :

```
Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/
invocations" -Method Post -Body '{"payload":"hello world!"}' -ContentType
 "application/json"
```

3. Obtenez l'ID du conteneur.

```
docker ps
```

4. Utilisez la commande docker kill pour arrêter le conteneur. Dans cette commande, remplacez `3766c4ab331c` par l'ID du conteneur de l'étape précédente.

```
docker kill 3766c4ab331c
```

Déploiement de l'image

Pour charger l'image sur Amazon RIE et créer la fonction Lambda

1. Exécutez la commande get-login-password pour authentifier la CLI Docker auprès de votre registre Amazon ECR.
   - Définissez la `--region` valeur à l' Région AWS endroit où vous souhaitez créer le référentiel Amazon ECR.
   - `111122223333`Remplacez-le par votre Compte AWS identifiant.

```
aws ecr get-login-password --region us-east-1 | docker login --username AWS --
password-stdin 111122223333.dkr.ecr.us-east-1.amazonaws.com
```

2. Créez un référentiel dans Amazon ECR à l'aide de la commande create-repository.

```
aws ecr create-repository --repository-name hello-world --region us-east-1 --image-
scanning-configuration scanOnPush=true --image-tag-mutability MUTABLE
```

> **Note**
>
> Le référentiel Amazon ECR doit être Région AWS identique à la fonction Lambda.

En cas de succès, vous obtenez une réponse comme celle-ci :

```
{
    "repository": {
        "repositoryArn": "arn:aws:ecr:us-east-1:111122223333:repository/hello-
world",
        "registryId": "111122223333",
        "repositoryName": "hello-world",
        "repositoryUri": "111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-
world",
        "createdAt": "2023-03-09T10:39:01+00:00",
        "imageTagMutability": "MUTABLE",
        "imageScanningConfiguration": {
            "scanOnPush": true
        },
        "encryptionConfiguration": {
            "encryptionType": "AES256"
        }
    }
}
```

3. Copiez le `repositoryUri` à partir de la sortie de l'étape précédente.
4. Exécutez la commande docker tag pour étiqueter votre image locale dans votre référentiel Amazon ECR en tant que dernière version. Dans cette commande :

- `docker-image:test` est le nom et la balise de votre image Docker. Il s'agit du nom et de la balise de l'image que vous avez spécifiés dans la commande `docker build`.
- Remplacez `<ECRrepositoryUri>` par l'`repositoryUri` que vous avez copié. Assurez-vous d'inclure `:latest` à la fin de l'URI.

```
docker tag docker-image:test <ECRrepositoryUri>:latest
```

Exemple :

```
docker tag docker-image:test 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

5. Exécutez la commande docker push pour déployer votre image locale dans le référentiel Amazon ECR. Assurez-vous d'inclure `:latest` à la fin de l'URI du référentiel.

```
docker push 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

6. Créez un rôle d'exécution pour la fonction, si vous n'en avez pas déjà un. Vous aurez besoin de l'Amazon Resource Name (ARN) du rôle à l'étape suivante.
7. Créez la fonction Lambda. Pour `ImageUri`, indiquez l'URI du référentiel mentionné précédemment. Assurez-vous d'inclure `:latest` à la fin de l'URI.

```
aws lambda create-function \
  --function-name hello-world \
  --package-type Image \
  --code ImageUri=111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \
  --role arn:aws:iam::111122223333:role/lambda-ex
```

> **Note**
>
> Vous pouvez créer une fonction en utilisant une image d'un autre AWS compte, à condition que l'image se trouve dans la même région que la fonction Lambda. Pour plus d'informations, consultez Autorisations entre comptes Amazon ECR.

8. Invoquer la fonction.

```
aws lambda invoke --function-name hello-world response.json
```

Vous devriez obtenir une réponse comme celle-ci :

```
{
  "ExecutedVersion": "$LATEST",
  "StatusCode": 200
}
```

9. Pour voir la sortie de la fonction, consultez le fichier `response.json`.

Pour mettre à jour le code de la fonction, vous devez recréer l'image, charger la nouvelle image dans le référentiel Amazon ECR, puis utiliser la commande update-function-code pour déployer l'image dans la fonction Lambda.

Lambda résout l'étiquette d'image en hachage d'image spécifique. Cela signifie que si vous pointez la balise d'image qui a été utilisée pour déployer la fonction vers une nouvelle image dans Amazon ECR, Lambda ne met pas automatiquement à jour la fonction pour utiliser la nouvelle image.

Pour déployer la nouvelle image sur la même fonction Lambda, vous devez utiliser la commande update-function-code, même si la balise d'image dans Amazon ECR reste la même. Dans l'exemple suivant, l'option `--publish` crée une version de la fonction à l'aide de l'image du conteneur mise à jour.

```
aws lambda update-function-code \
  --function-name hello-world \
  --image-uri 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \
  --publish
```

Utilisation d'une autre image de base avec le client d'interface d'exécution

Si vous utilisez une image OS-only de base ou une image de base alternative, vous devez inclure le client d'interface d'exécution dans votre image. Le client d'interface d'exécution étend leAPI de runtime, qui gère l'interaction entre Lambda et votre code de fonction.

Installez le client Node.js d'interface d'exécution à l'aide du gestionnaire de packages npm :

```
npm install aws-lambda-ric
```

Vous pouvez également télécharger le client Node.js d'interface d'exécution depuis GitHub.

L'exemple suivant montre comment créer une image de conteneur pour Node.js utiliser une image non AWS basique. L'exemple Dockerfile utilise une image de base `bookworm`. Le Dockerfile inclut le client d'interface d'exécution.

Conditions préalables

Pour exécuter la procédure indiquée dans cette section, vous devez satisfaire aux exigences suivantes :

- AWS CLI version 2
- Docker (version minimale 25.0.0)
- Le plug-in buildx Docker.
- Node.js

Création d'une image à partir d'une image de base alternative

Pour créer une image de conteneur à partir d'un objet autre que AWS image de base

1. Créez un répertoire pour le projet, puis passez à ce répertoire.

   ```
   mkdir example
   cd example
   ```

2. Créez un nouveau Node.js projet avec`npm`. Appuyez sur `Enter` pour accepter les options par défaut fournies dans l'expérience interactive.

   ```
   npm init
   ```

3. Créez un nouveau fichier appelé `index.js`. Vous pouvez ajouter l'exemple de code de fonction suivant au fichier pour le tester, ou utiliser le vôtre.

   Example Gestionnaire CommonJS

   ```
   exports.handler = async (event) => {
       const response = {
           statusCode: 200,
           body: JSON.stringify('Hello from Lambda!'),
       };
   ```

```
    return response;
};
```

4. Créez un nouveau fichier Docker. Le Dockerfile suivant utilise une image de base `bookworm` au lieu d'une image de base AWS. Le Dockerfile inclut le client d'interface d'exécution, ce qui rend l'image compatible avec Lambda. Le Dockerfile utilise une création à plusieurs étapes.

   La première étape crée une image de construction, qui est un Node.js environnement standard dans lequel les dépendances de la fonction sont installées. La deuxième étape crée une image plus fine qui inclut le code de la fonction et ses dépendances. Cela permet de réduire la taille de l'image finale.

   - Définissez la propriété `FROM` pour l'identifiant de l'image de base.
   - Utilisez la commande `COPY` pour copier le code de la fonction et les dépendances de l'exécution.
   - Définissez le `ENTRYPOINT` sur le module que vous souhaitez que le conteneur Docker exécute lorsqu'il démarre. Dans ce cas, le module est le client d'interface d'exécution.
   - Définir l'argument `CMD` pour le gestionnaire de la fonction Lambda.

   Notez que l'exemple de Dockerfile n'inclut pas d'instruction USER. Lorsque vous déployez une image de conteneur sur Lambda, Lambda définit automatiquement un utilisateur Linux par défaut disposant d'autorisations de moindre privilège. Ceci est différent du comportement standard de Docker qui est défini par défaut par l'utilisateur `root` lorsqu'aucune instruction USER n'est fournie.

   Example Dockerfile

```
# Define custom function directory
ARG FUNCTION_DIR="/function"

FROM node:20-bookworm as build-image

# Include global arg in this stage of the build
ARG FUNCTION_DIR

# Install build dependencies
RUN apt-get update && \
    apt-get install -y \
    g++ \
```

```
    make \
    cmake \
    unzip \
    libcurl4-openssl-dev

# Copy function code
RUN mkdir -p ${FUNCTION_DIR}
COPY . ${FUNCTION_DIR}

WORKDIR ${FUNCTION_DIR}

# Install Node.js dependencies
RUN npm install

# Install the runtime interface client
RUN npm install aws-lambda-ric

# Grab a fresh slim copy of the image to reduce the final size
FROM node:20-bookworm-slim

# Required for Node runtimes which use npm@8.6.0+ because
# by default npm writes logs under /home/.npm and Lambda fs is read-only
ENV NPM_CONFIG_CACHE=/tmp/.npm

# Include global arg in this stage of the build
ARG FUNCTION_DIR

# Set working directory to function root directory
WORKDIR ${FUNCTION_DIR}

# Copy in the built dependencies
COPY --from=build-image ${FUNCTION_DIR} ${FUNCTION_DIR}

# Set runtime interface client as default command for the container runtime
ENTRYPOINT ["/usr/local/bin/npx", "aws-lambda-ric"]
# Pass the name of the function handler as an argument to the runtime
CMD ["index.handler"]
```

5. Générez l'image Docker à l'aide de la commande docker build. L'exemple suivant nomme l'image `docker-image` et lui donne la balise `test`. Pour rendre votre image compatible avec Lambda, vous devez utiliser l'option `--provenance=false`.

```
docker buildx build --platform linux/amd64 --provenance=false -t docker-image:test
 .
```

> **Note**
>
> La commande spécifie l'option `--platform linux/amd64` pour garantir la compatibilité de votre conteneur avec l'environnement d'exécution Lambda, quelle que soit l'architecture de votre machine de génération. Si vous avez l'intention de créer une fonction Lambda à l'aide de l'architecture du jeu d'instructions ARM64, veillez à modifier la commande pour utiliser plutôt l'option `--platform linux/arm64`.

(Facultatif) Testez l'image localement

Utilisez l'émulateur d'interface d'exécution pour tester l'image localement. Vous pouvez intégrer l'émulateur dans votre image ou utiliser la procédure suivante pour l'installer sur votre machine locale.

Pour installer et exécuter l'émulateur d'interface d'exécution sur votre ordinateur local

1. Depuis le répertoire de votre projet, exécutez la commande suivante pour télécharger l'émulateur d'interface d'exécution (architecture x86-64) GitHub et l'installer sur votre machine locale.

   Linux/macOS

   ```
   mkdir -p ~/.aws-lambda-rie && \
       curl -Lo ~/.aws-lambda-rie/aws-lambda-rie https://github.com/aws/aws-lambda-
   runtime-interface-emulator/releases/latest/download/aws-lambda-rie && \
       chmod +x ~/.aws-lambda-rie/aws-lambda-rie
   ```

   Pour installer l'émulateur arm64, remplacez l'URL du GitHub référentiel dans la commande précédente par la suivante :

   ```
   https://github.com/aws/aws-lambda-runtime-interface-emulator/releases/latest/
   download/aws-lambda-rie-arm64
   ```

PowerShell

```
$dirPath = "$HOME\.aws-lambda-rie"
if (-not (Test-Path $dirPath)) {
    New-Item -Path $dirPath -ItemType Directory
}

$downloadLink = "https://github.com/aws/aws-lambda-runtime-interface-emulator/
releases/latest/download/aws-lambda-rie"
$destinationPath = "$HOME\.aws-lambda-rie\aws-lambda-rie"
Invoke-WebRequest -Uri $downloadLink -OutFile $destinationPath
```

Pour installer l'émulateur arm64, remplacez `$downloadLink` par ce qui suit :

```
https://github.com/aws/aws-lambda-runtime-interface-emulator/releases/latest/
download/aws-lambda-rie-arm64
```

2. Démarrez votre image Docker à l'aide de la commande docker run. Notez ce qui suit :

   - `docker-image` est le nom de l'image et `test` est la balise.
   - `/usr/local/bin/npx aws-lambda-ric index.handler` est le `ENTRYPOINT` suivi du `CMD` depuis votre Dockerfile.

Linux/macOS

```
docker run --platform linux/amd64 -d -v ~/.aws-lambda-rie:/aws-lambda -p
 9000:8080 \
    --entrypoint /aws-lambda/aws-lambda-rie \
    docker-image:test \
        /usr/local/bin/npx aws-lambda-ric index.handler
```

PowerShell

```
docker run --platform linux/amd64 -d -v "$HOME\.aws-lambda-rie:/aws-lambda" -p
 9000:8080 `
--entrypoint /aws-lambda/aws-lambda-rie `
docker-image:test `
    /usr/local/bin/npx aws-lambda-ric index.handler
```

Cette commande exécute l'image en tant que conteneur et crée un point de terminaison local à `localhost:9000/2015-03-31/functions/function/invocations`.

> **Note**
>
> Si vous avez créé l'image Docker pour l'architecture du jeu d'instructions ARM64, veillez à utiliser l'option `--platform linux/arm64` plutôt que `--platform linux/amd64`.

3. Publiez un événement au point de terminaison local.

   Linux/macOS

   Sous Linux et macOS, exécutez la commande `curl` suivante :

   ```
   curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d '{}'
   ```

   Cette commande invoque la fonction avec un événement vide et renvoie une réponse. Si vous utilisez votre propre code de fonction plutôt que l'exemple de code de fonction, vous pouvez invoquer la fonction avec une charge utile JSON. Exemple :

   ```
   curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d
    '{"payload":"hello world!"}'
   ```

   PowerShell

   Dans PowerShell, exécutez la `Invoke-WebRequest` commande suivante :

   ```
   Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/
   invocations" -Method Post -Body '{}' -ContentType "application/json"
   ```

   Cette commande invoque la fonction avec un événement vide et renvoie une réponse. Si vous utilisez votre propre code de fonction plutôt que l'exemple de code de fonction, vous pouvez invoquer la fonction avec une charge utile JSON. Exemple :

   ```
   Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/
   invocations" -Method Post -Body '{"payload":"hello world!"}' -ContentType
    "application/json"
   ```

4. Obtenez l'ID du conteneur.

```
docker ps
```

5. Utilisez la commande docker kill pour arrêter le conteneur. Dans cette commande, remplacez `3766c4ab331c` par l'ID du conteneur de l'étape précédente.

```
docker kill 3766c4ab331c
```

Déploiement de l'image

Pour charger l'image sur Amazon RIE et créer la fonction Lambda

1. Exécutez la commande get-login-password pour authentifier la CLI Docker auprès de votre registre Amazon ECR.

   - Définissez la `--region` valeur à l' Région AWS endroit où vous souhaitez créer le référentiel Amazon ECR.
   - `111122223333`Remplacez-le par votre Compte AWS identifiant.

```
aws ecr get-login-password --region us-east-1 | docker login --username AWS --
password-stdin 111122223333.dkr.ecr.us-east-1.amazonaws.com
```

2. Créez un référentiel dans Amazon ECR à l'aide de la commande create-repository.

```
aws ecr create-repository --repository-name hello-world --region us-east-1 --image-
scanning-configuration scanOnPush=true --image-tag-mutability MUTABLE
```

> **Note**
>
> Le référentiel Amazon ECR doit être Région AWS identique à la fonction Lambda.

En cas de succès, vous obtenez une réponse comme celle-ci :

```
{
    "repository": {
```

```
        "repositoryArn": "arn:aws:ecr:us-east-1:111122223333:repository/hello-
world",
        "registryId": "111122223333",
        "repositoryName": "hello-world",
        "repositoryUri": "111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-
world",
        "createdAt": "2023-03-09T10:39:01+00:00",
        "imageTagMutability": "MUTABLE",
        "imageScanningConfiguration": {
            "scanOnPush": true
        },
        "encryptionConfiguration": {
            "encryptionType": "AES256"
        }
    }
}
```

3. Copiez le `repositoryUri` à partir de la sortie de l'étape précédente.
4. Exécutez la commande docker tag pour étiqueter votre image locale dans votre référentiel Amazon ECR en tant que dernière version. Dans cette commande :

   - `docker-image:test` est le nom et la balise de votre image Docker. Il s'agit du nom et de la balise de l'image que vous avez spécifiés dans la commande `docker build`.
   - Remplacez <ECRrepositoryUri> par l'`repositoryUri` que vous avez copié. Assurez-vous d'inclure `:latest` à la fin de l'URI.

   ```
   docker tag docker-image:test <ECRrepositoryUri>:latest
   ```

   Exemple :

   ```
   docker tag docker-image:test 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-
   world:latest
   ```

5. Exécutez la commande docker push pour déployer votre image locale dans le référentiel Amazon ECR. Assurez-vous d'inclure `:latest` à la fin de l'URI du référentiel.

   ```
   docker push 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
   ```

6. Créez un rôle d'exécution pour la fonction, si vous n'en avez pas déjà un. Vous aurez besoin de l'Amazon Resource Name (ARN) du rôle à l'étape suivante.

7. Créez la fonction Lambda. Pour `ImageUri`, indiquez l'URI du référentiel mentionné précédemment. Assurez-vous d'inclure `:latest` à la fin de l'URI.

```
aws lambda create-function \
  --function-name hello-world \
  --package-type Image \
  --code ImageUri=111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \
  --role arn:aws:iam::111122223333:role/lambda-ex
```

> **Note**
>
> Vous pouvez créer une fonction en utilisant une image d'un autre AWS compte, à condition que l'image se trouve dans la même région que la fonction Lambda. Pour plus d'informations, consultez Autorisations entre comptes Amazon ECR.

8. Invoquer la fonction.

```
aws lambda invoke --function-name hello-world response.json
```

Vous devriez obtenir une réponse comme celle-ci :

```
{
  "ExecutedVersion": "$LATEST",
  "StatusCode": 200
}
```

9. Pour voir la sortie de la fonction, consultez le fichier `response.json`.

Pour mettre à jour le code de la fonction, vous devez recréer l'image, charger la nouvelle image dans le référentiel Amazon ECR, puis utiliser la commande update-function-code pour déployer l'image dans la fonction Lambda.

Lambda résout l'étiquette d'image en hachage d'image spécifique. Cela signifie que si vous pointez la balise d'image qui a été utilisée pour déployer la fonction vers une nouvelle image dans Amazon ECR, Lambda ne met pas automatiquement à jour la fonction pour utiliser la nouvelle image.

Pour déployer la nouvelle image sur la même fonction Lambda, vous devez utiliser la commande update-function-code, même si la balise d'image dans Amazon ECR reste la même. Dans l'exemple

suivant, l'option `--publish` crée une version de la fonction à l'aide de l'image du conteneur mise à jour.

```
aws lambda update-function-code \
  --function-name hello-world \
  --image-uri 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \
  --publish
```

Utilisation de couches pour les fonctions d' Node.js événement Lambda

Utilisez les couches Lambda pour empaqueter le code et les dépendances que vous souhaitez réutiliser dans plusieurs fonctions. Les couches contiennent généralement des dépendances de bibliothèque, une exécution personnalisée, ou des fichiers de configuration. La création d'une couche implique trois étapes générales :

1. Empaquetez le contenu de votre couche. Cela signifie créer une archive de fichiers .zip contenant les dépendances que vous souhaitez utiliser dans vos fonctions.
2. Créez la couche dans Lambda.
3. Ajoutez la couche à vos fonctions.

Rubriques

- Empaqueter le contenu de votre couche
- Créer la couche dans Lambda
- Ajouter la couche à votre fonction
- Exemple d'application

Empaqueter le contenu de votre couche

Pour créer une couche, regroupez vos packages dans une archive (fichier .zip) répondant aux exigences suivantes :

- Créez la couche en utilisant la même Node.js version que celle que vous prévoyez d'utiliser pour la fonction Lambda. Par exemple, si vous créez votre couche à l'aide de Node.js 24, utilisez le runtime Node.js 24 pour votre fonction.
- Le fichier .zip de votre couche doit utiliser l'une des structures de répertoires suivantes :
  - `nodejs/node_modules`
  - `nodejs/node`*X*`/node_modules`(où *X* est votre Node.js version, par exemple`node22`)

  Pour plus d'informations, consultez Chemins d'accès de couche pour chaque exécution Lambda.
- Les packages de votre couche doivent être compatibles avec Linux. Les fonctions Lambda s'exécutent sur Amazon Linux.

Vous pouvez créer des couches contenant des Node.js bibliothèques tierces installées avec `npm` (telles que `axios` ou`lodash`) ou vos propres JavaScript modules.

Third-party dépendances

Créer une couche à l'aide de packages npm

1. Créez la structure de répertoires requise et installez-y les packages directement :

   ```
   mkdir -p nodejs
   npm install --prefix nodejs lodash axios
   ```

   Cette commande installe les packages directement dans le répertoire `nodejs/node_modules`, qui correspond à la structure requise par Lambda.

   > **Note**
   >
   > Pour les packages avec des dépendances natives ou des composants binaires (comme sharp ou bcrypt), assurez-vous qu'ils sont compatibles avec l'environnement Linux Lambda et l'architecture de votre fonction. Vous devrez peut-être utiliser l'indicateur `--platform` :
   >
   > ```
   > npm install --prefix nodejs --platform=linux --arch=x64 sharp
   > ```
   >
   > Pour les dépendances natives plus complexes, vous devrez peut-être les compiler dans un environnement Linux qui correspond à l'environnement d'exécution Lambda. Vous pouvez utiliser Docker à cette fin.

2. Compressez le contenu de la couche :

   Linux/macOS

   ```
   zip -r layer.zip nodejs/
   ```

   PowerShell

   ```
   Compress-Archive -Path .\nodejs -DestinationPath .\layer.zip
   ```

La structure de répertoire de votre fichier .zip devrait se présenter comme suit :

```
nodejs/
### package.json
### package-lock.json
### node_modules/
    ### lodash/
    ### axios/
    ### (dependencies of the other packages)
```

> **Note**
>
> - Assurez-vous que votre fichier .zip inclut le répertoire `nodejs` au niveau racine avec `node_modules` à l'intérieur. Cette structure garantit que Lambda peut localiser et importer vos packages.
> - Les fichiers `package.json` et `package-lock.json` du répertoire `nodejs/` sont utilisés par npm pour la gestion des dépendances, mais ne sont pas requis par Lambda pour le fonctionnement des couches. Chaque package installé contient déjà son propre fichier `package.json` qui définit la manière dont Lambda importe le package.

JavaScript Modules personnalisés

Créer une couche à l'aide de votre propre code

1. Créez la structure de répertoires requise pour votre couche :

   ```
   mkdir -p nodejs/node_modules/validator
   cd nodejs/node_modules/validator
   ```

2. Créez un fichier `package.json` pour votre module personnalisé afin de définir comment il doit être importé :

   Example nodejs/node_modules/validator/package.json

   ```
   {
   ```

```
  "name": "validator",
  "version": "1.0.0",
  "type": "module",
  "main": "index.mjs"
}
```

3. Créez le fichier JavaScript de votre module :

   Example nodejs/node_modules/validator/index.mjs

```
export function validateOrder(orderData) {
  // Validates an order and returns formatted data
  const requiredFields = ['productId', 'quantity'];

  // Check required fields
  const missingFields = requiredFields.filter(field => !(field in orderData));
  if (missingFields.length > 0) {
    throw new Error(`Missing required fields: ${missingFields.join(', ')}`);
  }

  // Validate quantity
  const quantity = orderData.quantity;
  if (!Number.isInteger(quantity) || quantity < 1) {
    throw new Error('Quantity must be a positive integer');
  }

  // Format and return the validated data
  return {
    productId: String(orderData.productId),
    quantity: quantity,
    shippingPriority: orderData.priority || 'standard'
  };
}

export function formatResponse(statusCode, body) {
  // Formats the API response
  return {
    statusCode: statusCode,
    body: JSON.stringify(body)
  };
}
```

4. Compressez le contenu de la couche :

Linux/macOS

```
zip -r layer.zip nodejs/
```

PowerShell

```
Compress-Archive -Path .\nodejs -DestinationPath .\layer.zip
```

La structure de répertoire de votre fichier .zip devrait se présenter comme suit :

```
nodejs/
### node_modules/
    ### validator/
        ### package.json
        ### index.mjs
```

5. Dans votre fonction, importez et utilisez les modules. Exemple :

```
import { validateOrder, formatResponse } from 'validator';

export const handler = async (event) => {
  try {
    // Parse the order data from the event body
    const orderData = JSON.parse(event.body || '{}');

    // Validate and format the order
    const validatedOrder = validateOrder(orderData);

    return formatResponse(200, {
      message: 'Order validated successfully',
      order: validatedOrder
    });
  } catch (error) {
    if (error instanceof Error && error.message.includes('Missing required
 fields')) {
      return formatResponse(400, {
        error: error.message
      });
    }
```

```
    return formatResponse(500, {
      error: 'Internal server error'
    });
  }
};
```

Vous pouvez utiliser l'événement de test suivant afin d'invoquer la fonction :

```
{
    "body": "{\"productId\": \"ABC123\", \"quantity\": 2, \"priority\": \"express
\"}"
}
```

Réponse attendue :

```
{
  "statusCode": 200,
  "body": "{\"message\":\"Order validated successfully\",\"order\":{\"productId\":
\"ABC123\",\"quantity\":2,\"shippingPriority\":\"express\"}}"
}
```

Créer la couche dans Lambda

Vous pouvez publier votre couche à l'aide de la console Lambda AWS CLI ou de la console Lambda.

AWS CLI

Exécutez la AWS CLI commande publish-layer-version pour créer la couche Lambda :

```
aws lambda publish-layer-version --layer-name my-layer --zip-file fileb://layer.zip
 --compatible-runtimes nodejs24.x
```

Le paramètre compatible runtimes est facultatif. Lorsqu'il est spécifié, Lambda utilise ce paramètre pour filtrer les couches dans la console Lambda.

Console

Pour créer une couche (console)

1. Ouvrez la page Couches de la console Lambda.
2. Sélectionnez Créer un calque.

3. Choisissez Charger un fichier .zip, puis chargez l'archive .zip que vous avez créée précédemment.
4. (Facultatif) Pour les environnements d'exécution compatibles, choisissez le Node.js moteur d'exécution correspondant à la Node.js version que vous avez utilisée pour créer votre couche.
5. Cliquez sur Créer.

Ajouter la couche à votre fonction

AWS CLI

Pour associer la couche à votre fonction, exécutez la commande update-function-configuration AWS CLI . Utilisez l'ARN de la couche pour le paramètre `--layers`. L'ARN doit spécifier la version (par exemple, `arn:aws:lambda:us-east-1:123456789012:layer:my-layer:1`). Pour plus d'informations, consultez Couches et versions de couches.

```
aws lambda update-function-configuration --function-name my-function --cli-binary-format raw-in-base64-out --layers "arn:aws:lambda:us-east-1:123456789012:layer:my-layer:1"
```

L'cli-binary-formatoption est obligatoire si vous utilisez AWS CLI la version 2. Pour faire de ce paramètre le paramètre par défaut, exécutez `aws configure set cli-binary-format raw-in-base64-out`. Pour plus d'informations, consultez les options de ligne de commande globales AWS CLI prises en charge dans le Guide de l'utilisateur AWS Command Line Interface version 2.

Console

Ajouter une couche à une fonction

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez la fonction.
3. Faites défiler jusqu'à la section Couches, puis choisissez Ajouter une couche.
4. Sous Choisir une couche, sélectionnez Couches personnalisées, puis choisissez votre couche.

> **Note**
>
> Si vous n'avez pas ajouté d'environnement d'exécution compatible lors de la création de la couche, celle-ci ne sera pas répertoriée ici. Vous pouvez spécifier l'ARN de la couche à la place.

5. Choisissez Ajouter.

Exemple d'application

Pour d'autres exemples d'utilisation des couches Lambda, consultez l'exemple d'application layer-nodejs dans le référentiel du Developer Guide. AWS Lambda GitHub Cette application inclut une couche qui contient la bibliothèque lodash. Après avoir créé la couche, vous pouvez déployer et invoquer la fonction correspondante pour confirmer que la couche fonctionne comme prévu.

Utilisation de l'objet de contexte Lambda pour récupérer les informations de la fonction Node.js d'événement

Lorsque Lambda exécute votre fonction, il transmet un objet contexte au gestionnaire. Cet objet fournit des méthodes et des propriétés fournissant des informations sur l'invocation, la fonction et l'environnement d'exécution.

Méthodes de contexte

- `getRemainingTimeInMillis()` – Renvoie le nombre de millisecondes restant avant l'expiration de l'exécution.

Propriétés du contexte

- `functionName` – Nom de la fonction Lambda.
- `functionVersion` – Version de la fonction.
- `invokedFunctionArn` – Amazon Resource Name (ARN) utilisé pour appeler la fonction. Indique si l'appelant a spécifié un numéro de version ou un alias.
- `memoryLimitInMB` – Quantité de mémoire allouée à la fonction.
- `awsRequestId` – Identifiant de la demande d'invocation.
- `logGroupName` – Groupe de journaux pour la fonction.
- `logStreamName` – Flux de journal de l'instance de fonction.
- `identity` – (applications mobiles) Informations sur l'identité Amazon Cognito qui a autorisé la demande.
  - `cognitoIdentityId` – Identité Amazon Cognito authentifiée.
  - `cognitoIdentityPoolId` – Groupe d'identités Amazon Cognito ayant autorisé l'invocation.
- `clientContext` – (applications mobiles) Contexte client fourni à Lambda par l'application client.
  - `client.installation_id`
  - `client.app_title`
  - `client.app_version_name`
  - `client.app_version_code`
  - `client.app_package_name`
  - `env.platform_version`
  - `env.platform`

  - `env.make`
  - `env.model`
  - `env.locale`
  - `custom` – Personnalisez les valeurs qui sont définies par l'application client.
- `callbackWaitsForEmptyEventLoop`— Par défaut (`true`), lors de l'utilisation d'un gestionnaire de fonctions basé sur le rappel, Lambda attend que la boucle d'événements soit vide après l'exécution du rappel avant de terminer l'appel de la fonction. Définissez cette valeur `false` sur pour envoyer la réponse et mettre fin à l'appel immédiatement après l'exécution du rappel au lieu d'attendre que la boucle d'événements soit vide. Les événements exceptionnels continuent de se dérouler lors de la prochaine invocation. Notez que Lambda prend en charge les gestionnaires de fonctions basés sur le rappel uniquement pour les environnements d'exécution Node.js 22 et antérieurs.

Dans l'exemple suivant, la fonction enregistre des informations de contexte et renvoie l'emplacement des journaux.

Example Fichier index.js

```
exports.handler = async function(event, context) {
  console.log('Remaining time: ', context.getRemainingTimeInMillis())
  console.log('Function name: ', context.functionName)
  return context.logStreamName
}
```

Enregistrez et surveillez les fonctions des Node.js événements Lambda

AWS Lambda surveille automatiquement les fonctions d'événement Lambda en votre nom et envoie les journaux à Amazon. CloudWatch Votre fonction est fournie avec un groupe de CloudWatch journaux Logs et un flux de journaux pour chaque instance de votre fonction. L'environnement d'exécution Lambda envoie des informations sur chaque invocation au flux de journaux et transmet les journaux et autres sorties provenant du code de votre fonction. Pour plus d'informations, consultez Envoi des journaux des fonctions d'événements Lambda aux journaux CloudWatch.

Cette page explique comment générer une sortie de journal à partir du code de votre fonction Lambda et comment accéder aux journaux à l'aide de la AWS Command Line Interface console Lambda ou de la console. CloudWatch

Sections

- Création d'une fonction qui renvoie des journaux
- Utilisation des commandes de journalisation avancées de Lambda avec Node.js
- Affichage des journaux dans la console Lambda
- Afficher les journaux dans la CloudWatch console
- Afficher les journaux à l'aide du AWS Command Line Interface (AWS CLI)
- Suppression de journaux

Création d'une fonction qui renvoie des journaux

Pour générer les journaux à partir de votre code de fonction, vous pouvez utiliser des méthodes sur l'objet console ou n'importe quelle bibliothèque de journalisation qui écrit dans `stdout` ou `stderr`. L'exemple suivant consigne les valeurs des variables d'environnement et l'objet d'événement.

> **Note**
>
> Nous vous recommandons d'utiliser des techniques telles que la validation des entrées et le codage des sorties lors de la journalisation des entrées. Si vous journalisez directement les données d'entrée, un attaquant peut utiliser votre code pour rendre les altérations difficiles à détecter, falsifier des entrées de journal ou contourner les moniteurs de journal. Pour plus d'informations, consultez Improper Output Neutralization for Logs dans la Common Weakness Enumeration.

Example Fichier index.js – Journalisation

```
exports.handler = async function(event, context) {
  console.log("ENVIRONMENT VARIABLES\n" + JSON.stringify(process.env, null, 2))
  console.info("EVENT\n" + JSON.stringify(event, null, 2))
  console.warn("Event not processed.")
  return context.logStreamName
}
```

Example format des journaux

```
START RequestId: c793869b-ee49-115b-a5b6-4fd21e8dedac Version: $LATEST
2019-06-07T19:11:20.562Z c793869b-ee49-115b-a5b6-4fd21e8dedac INFO ENVIRONMENT
 VARIABLES
{
  "AWS_LAMBDA_FUNCTION_VERSION": "$LATEST",
  "AWS_LAMBDA_LOG_GROUP_NAME": "/aws/lambda/my-function",
  "AWS_LAMBDA_LOG_STREAM_NAME": "2019/06/07/[$LATEST]e6f4a0c4241adcd70c262d34c0bbc85c",
  "AWS_EXECUTION_ENV": "AWS_Lambda_nodejs12.x",
  "AWS_LAMBDA_FUNCTION_NAME": "my-function",
  "PATH": "/var/lang/bin:/usr/local/bin:/usr/bin/:/bin:/opt/bin",
  "NODE_PATH": "/opt/nodejs/node10/node_modules:/opt/nodejs/node_modules:/var/runtime/
node_modules",
  ...
}
2019-06-07T19:11:20.563Z c793869b-ee49-115b-a5b6-4fd21e8dedac INFO EVENT
{
  "key": "value"
}
2019-06-07T19:11:20.564Z c793869b-ee49-115b-a5b6-4fd21e8dedac WARN Event not processed.
END RequestId: c793869b-ee49-115b-a5b6-4fd21e8dedac
REPORT RequestId: c793869b-ee49-115b-a5b6-4fd21e8dedac Duration: 128.83 ms Billed
 Duration: 296 ms Memory Size: 128 MB Max Memory Used: 74 MB Init Duration: 166.62 ms
 XRAY TraceId: 1-5d9d007f-0a8c7fd02xmpl480aed55ef0 SegmentId: 3d752xmpl1bbe37e Sampled:
 true
```

Le Node.js moteur d'exécution enregistre les `REPORT` lignes `START``END`, et pour chaque appel. Il ajoute un horodatage, un ID de demande et un niveau de journalisation sur chaque entrée consignée par la fonction. La ligne de rapport fournit les détails suivants.

Champs de données de la ligne REPORT

- RequestId— L'identifiant de demande unique pour l'invocation.
- Duration – Temps que la méthode de gestion du gestionnaire de votre fonction a consacré au traitement de l'événement.
- Billed Duration : temps facturé pour l'invocation.
- Memory Size – Quantité de mémoire allouée à la fonction.
- Max Memory Used – Quantité de mémoire utilisée par la fonction. Lorsque les appels partagent un environnement d'exécution, Lambda indique la mémoire maximale utilisée pour toutes les invocations. Ce comportement peut entraîner une valeur signalée plus élevée que prévu.
- Init Duration : pour la première requête servie, temps qu'il a pris à l'exécution charger la fonction et exécuter le code en dehors de la méthode du gestionnaire.
- XRAY TraceId — Pour les demandes suivies, l'ID de AWS X-Ray trace.
- SegmentId— Pour les demandes suivies, l'ID X-Ray du segment.
- Sampled – Pour les demandes suivies, résultat de l'échantillonnage.

Vous pouvez consulter les journaux dans la console Lambda, dans la console CloudWatch Logs ou depuis la ligne de commande.

Utilisation des commandes de journalisation avancées de Lambda avec Node.js

Pour mieux contrôler la manière dont les journaux de vos fonctions sont capturés, traités et consommés, vous pouvez configurer les options de journalisation suivantes pour les environnements d' Node.js exécution pris en charge :

- Format de journal : choisissez entre le format texte brut et le format JSON structuré pour les journaux de votre fonction
- Niveau de journalisation : pour les journaux au format JSON, choisissez le niveau de détail des journaux que Lambda envoie à Amazon CloudWatch, par exemple ERROR, DEBUG ou INFO
- Groupe de journaux : choisissez le groupe de CloudWatch journaux auquel votre fonction envoie les journaux

Pour plus d'informations sur ces options de journalisation et pour savoir comment configurer votre fonction pour les utiliser, consultez the section called "Configuration de contrôles de journalisation avancés pour les fonctions d'événement Lambda".

Pour utiliser le format de journal et les options de niveau de journal avec vos fonctions Node.js Lambda, consultez les instructions des sections suivantes.

Utilisation de journaux JSON structurés avec Node.js

Si vous sélectionnez JSON pour le format de journal de votre fonction, Lambda envoie les résultats des journaux en utilisant les méthodes de console`console.trace`,,,`console.debug`, `console.log` `console.info`console.error, et `console.warn` vers CloudWatch sous forme de JSON structuré. Chaque objet de journal JSON contient au moins quatre paires clé-valeur avec les clés suivantes :

- `"timestamp"` - heure à laquelle le message de journal a été généré
- `"level"` - niveau de journalisation attribué au message
- `"message"` - contenu du message de journal
- `"requestId"` - identifiant unique de la demande pour l'invocation de la fonction

Selon la méthode de journalisation utilisée par votre fonction, cet objet JSON peut également contenir des paires de clés supplémentaires. Par exemple, si votre fonction utilise des méthodes `console` pour enregistrer les objets d'erreur à l'aide de plusieurs arguments, l'objet JSON contiendra des paires clé-valeur supplémentaires avec les clés `errorMessage`, `errorType` et `stackTrace`.

Si votre code utilise déjà une autre bibliothèque de journalisation, telle que Powertools for AWS Lambda, pour produire des journaux structurés en JSON, vous n'avez pas besoin d'apporter de modifications. Lambda n'encode pas deux fois les journaux déjà codés au format JSON, de sorte que les journaux d'application de votre fonction continuent d'être capturés comme avant.

Pour plus d'informations sur l'utilisation du package Powertools for AWS Lambda logging afin de créer des journaux structurés JSON au moment de l' Node.js exécution, consultezthe section called “Logging”.

Exemple de sorties de journal au format JSON

Les exemples suivants montrent comment les différentes sorties de journal générées à l'aide `console` des méthodes avec des arguments uniques et multiples sont capturées dans CloudWatch Logs lorsque vous définissez le format de journal de votre fonction sur JSON.

Le premier exemple utilise la méthode `console.error` pour générer une chaîne simple.

Example Node.js code de journalisation

```
export const handler = async (event) => {
  console.error("This is a warning message");
  ...
}
```

Example Enregistrement de journaux JSON

```
{
    "timestamp":"2025-11-01T00:21:51.358Z",
    "level":"ERROR",
    "message":"This is a warning message",
    "requestId":"93f25699-2cbf-4976-8f94-336a0aa98c6f"
}
```

Vous pouvez également générer des messages de journal structurés plus complexes en utilisant un ou plusieurs arguments avec les méthodes `console`. Dans l'exemple suivant, vous pouvez utiliser `console.log` pour générer deux paires clé-valeur avec un seul argument. Notez que le `"message"` champ de l'objet JSON envoyé par Lambda à CloudWatch Logs n'est pas stringifié.

Example Node.js code de journalisation

```
export const handler = async (event) => {
  console.log({data: 12.3, flag: false});
  ...
}
```

Example Enregistrement de journaux JSON

```
{
    "timestamp": "2025-12-08T23:21:04.664Z",
    "level": "INFO",
    "requestId": "405a4537-9226-4216-ac59-64381ec8654a",
    "message": {
        "data": 12.3,
        "flag": false
    }
}
```

Dans l'exemple suivant, vous utilisez à nouveau la méthode `console.log` pour créer une sortie de journal. Cette fois, la méthode prend deux arguments, une carte contenant deux paires clé-valeur et une chaîne d'identification. Notez que dans ce cas, parce que vous avez fourni deux arguments, Lambda stringifie le champ `"message"`.

Example Node.js code de journalisation

```
export const handler = async (event) => {
  console.log('Some object - ', {data: 12.3, flag: false});
  ...
}
```

Example Enregistrement de journaux JSON

```
{
    "timestamp": "2025-12-08T23:21:04.664Z",
    "level": "INFO",
    "requestId": "405a4537-9226-4216-ac59-64381ec8654a",
    "message": "Some object -  { data: 12.3, flag: false }"
}
```

Lambda attribue les sorties générées à l'aide de `console.log` du niveau de journalisation INFO.

Le dernier exemple montre comment les objets d'erreur peuvent être générés dans CloudWatch Logs à l'aide `console` des méthodes. Notez que lorsque vous enregistrez des objets d'erreur à l'aide de plusieurs arguments, Lambda ajoute les champs `errorMessage`, `errorType` et `stackTrace` à la sortie du journal.

Example Node.js code de journalisation

```
export const handler = async (event) => {
  let e1 = new ReferenceError("some reference error");
  let e2 = new SyntaxError("some syntax error");
  console.log(e1);
  console.log("errors logged - ", e1, e2);
};
```

Example Enregistrement de journaux JSON

```
{
```

```
    "timestamp": "2025-12-08T23:21:04.632Z",
    "level": "INFO",
    "requestId": "405a4537-9226-4216-ac59-64381ec8654a",
    "message": {
        "errorType": "ReferenceError",
        "errorMessage": "some reference error",
        "stackTrace": [
            "ReferenceError: some reference error",
            "    at Runtime.handler (file:///var/task/index.mjs:3:12)",
            "    at Runtime.handleOnceNonStreaming (file:///var/runtime/
index.mjs:1173:29)"
        ]
    }
}

{
    "timestamp": "2025-12-08T23:21:04.646Z",
    "level": "INFO",
    "requestId": "405a4537-9226-4216-ac59-64381ec8654a",
    "message": "errors logged -  ReferenceError: some reference error
\n    at Runtime.handler (file:///var/task/index.mjs:3:12)\n    at
 Runtime.handleOnceNonStreaming
    (file:///var/runtime/index.mjs:1173:29) SyntaxError: some syntax
 error\n    at Runtime.handler (file:///var/task/index.mjs:4:12)\n    at
 Runtime.handleOnceNonStreaming
    (file:///var/runtime/index.mjs:1173:29)",
    "errorType": "ReferenceError",
    "errorMessage": "some reference error",
    "stackTrace": [
        "ReferenceError: some reference error",
        "    at Runtime.handler (file:///var/task/index.mjs:3:12)",
        "    at Runtime.handleOnceNonStreaming (file:///var/runtime/index.mjs:1173:29)"
    ]
}
```

Lors de la journalisation de plusieurs types d'erreur, les champs supplémentaires `errorMessage`, `errorType`, et `stackTrace` sont extraits du premier type d'erreur fourni à la méthode `console`.

Utilisation de bibliothèques clientes au format métrique intégré (EMF) avec des journaux JSON structurés

AWS fournit des bibliothèques clientes open source Node.js que vous pouvez utiliser pour créer des journaux au format métrique intégré (EMF). Si vous avez des fonctions existantes qui utilisent ces

bibliothèques et que vous modifiez le format de journal de votre fonction en JSON, CloudWatch il est possible que les métriques émises par votre code ne soient plus reconnues.

Si votre code émet actuellement des journaux EMF directement en utilisant `console.log` ou en utilisant Powertools for AWS Lambda (TypeScript), CloudWatch il est également incapable de les analyser si vous modifiez le format de journal de votre fonction en JSON.

> **Important**
>
> Pour vous assurer que les journaux EMF de vos fonctions continuent d'être correctement analysés CloudWatch, mettez à jour vos bibliothèques EMF et Powertools pour les AWS Lambda bibliothèques avec les dernières versions. Si vous passez au format de journal JSON, nous vous recommandons également d'effectuer des tests pour garantir la compatibilité avec les métriques intégrées de votre fonction. Si votre code émet des journaux EMF directement à l'aide de `console.log`, modifiez votre code pour qu'il affiche directement ces métriques vers `stdout`, comme indiqué dans l'exemple de code suivant.

Example code émettant des métriques intégrées vers **`stdout`**

```
process.stdout.write(JSON.stringify(
    {
        "_aws": {
            "Timestamp": Date.now(),
            "CloudWatchMetrics": [{
                "Namespace": "lambda-function-metrics",
                "Dimensions": [["functionVersion"]],
                "Metrics": [{
                    "Name": "time",
                    "Unit": "Milliseconds",
                    "StorageResolution": 60
                }]
            }]
        },
        "functionVersion": "$LATEST",
        "time": 100,
        "requestId": context.awsRequestId
    }
) + "\n")
```

Utilisation du filtrage au niveau du journal avec Node.js

AWS Lambda Pour filtrer les journaux de votre application en fonction de leur niveau de journalisation, votre fonction doit utiliser des journaux au format JSON. Vous pouvez effectuer cette opération de deux façons :

- Créez des sorties de journal à l'aide des méthodes de console standard et configurez votre fonction pour utiliser le format de journal JSON. AWS Lambda filtre ensuite les sorties de votre journal à l'aide de la paire clé-valeur « niveau » de l'objet JSON décrit dansthe section called “Utilisation de journaux JSON structurés avec Node.js”. Pour savoir comment configurer le format de journal de votre fonction, consultezthe section called “Configuration de contrôles de journalisation avancés pour les fonctions d'événement Lambda”.
- Utilisez une autre bibliothèque ou méthode de journalisation pour créer des journaux structurés JSON dans votre code qui incluent une paire clé-valeur « niveau » définissant le niveau de sortie du journal. Par exemple, vous pouvez utiliser Powertools pour générer des sorties AWS Lambda de journal structurées JSON à partir de votre code. Consultez the section called “Logging” pour en savoir plus sur l'utilisation de Powertools avec le moteur Node.js d'exécution.

  Pour que Lambda puisse filtrer les journaux de votre fonction, vous devez également inclure une paire `"timestamp"` clé-valeur dans la sortie de votre journal JSON. L’heure doit être spécifiée dans un format d’horodatage RFC 3339 valide. Si vous ne fournissez pas d'horodatage valide, Lambda attribue au journal le niveau INFO et ajoute un horodatage pour vous.

Lorsque vous configurez votre fonction pour utiliser le filtrage au niveau des journaux, vous sélectionnez le niveau de journaux que vous souhaitez envoyer AWS Lambda à CloudWatch Logs parmi les options suivantes :

Niveau de journalisation	Utilisation standard
TRACE (le plus détaillé)	Les informations les plus précises utilisées pour tracer le chemin d’exécution de votre code
DEBUG	Informations détaillées pour le débogage du système
INFO	Messages qui enregistrent le fonctionnement normal de votre fonction

Niveau de journalisation	Utilisation standard
WARN	Messages concernant des erreurs potentiel les susceptibles d'entraîner un comportement inattendu si elles ne sont pas traitées
ERROR	Messages concernant les problèmes qui empêchent le code de fonctionner comme prévu
FATAL (moindre détail)	Messages relatifs à des erreurs graves entraînant l’arrêt du fonctionnement de l’applica tion

Lambda envoie les journaux du niveau sélectionné et d'un niveau inférieur à. CloudWatch Par exemple, si vous configurez un niveau de journalisation WARN, Lambda envoie des journaux correspondant aux niveaux WARN, ERROR et FATAL.

Affichage des journaux dans la console Lambda

Vous pouvez utiliser la console Lambda pour consulter les résultats du journal après avoir invoqué une fonction d'événement Lambda.

Si votre code peut être testé à partir de l'éditeur de code intégré, vous trouverez des journaux dans les résultats d'exécution. Lorsque vous utilisez la fonctionnalité de test de la console pour appeler une fonction, vous trouverez la sortie du journal dans la section Détails.

Afficher les journaux dans la CloudWatch console

Vous pouvez utiliser la CloudWatch console Amazon pour consulter les journaux de toutes les invocations de la fonction d'événement Lambda.

Pour afficher les journaux sur la CloudWatch console

1. Ouvrez la page Groupes de journaux sur la CloudWatch console.
2. Choisissez le groupe de journaux pour votre fonction (/aws/lambda/***your-function-name***).
3. Choisissez un flux de journaux.

Chaque flux de journal correspond à une instance de votre fonction. Un flux de journal apparaît lorsque vous mettez à jour votre fonction Lambda et lorsque des instances supplémentaires sont créées pour gérer les appels simultanés. Pour trouver les journaux d'un appel spécifique, nous vous recommandons d'instrumenter votre fonction avec. AWS X-Ray X-Ray enregistre les détails de la demande et du flux de log dans le traçage.

Afficher les journaux à l'aide du AWS Command Line Interface (AWS CLI)

AWS CLI Il s'agit d'un outil open source que vous pouvez utiliser pour interagir avec les AWS services à l'aide de commandes dans votre interface de ligne de commande. Pour effectuer les étapes de cette section, vous devez disposer de la version 2 de l'AWS CLI.

Vous pouvez utiliser AWS CLI pour récupérer les journaux d'une invocation à l'aide de l'option de commande `--log-type`. La réponse inclut un champ `LogResult` qui contient jusqu'à 4 Ko de journaux codés en base64 provenant de l'invocation.

Example récupérer un ID de journal

L'exemple suivant montre comment récupérer un ID de journal à partir du champ `LogResult` d'une fonction nommée `my-function`.

```
aws lambda invoke --function-name my-function out --log-type Tail
```

Vous devriez voir la sortie suivante:

```
{
    "StatusCode": 200,
    "LogResult":
 "U1RBUlQgUmVxdWVzdElkOiA4N2QwNDRiOC1mMTU0LTExZTgtOGNkYS0yOTc0YzVlNGZiMjEgVmVyc2lvb...",
    "ExecutedVersion": "$LATEST"
}
```

Example décoder les journaux

Dans la même invite de commandes, utilisez l'utilitaire `base64` pour décoder les journaux. L'exemple suivant montre comment récupérer les journaux encodés en base64 pour `my-function`.

```
aws lambda invoke --function-name my-function out --log-type Tail \
--query 'LogResult' --output text --cli-binary-format raw-in-base64-out | base64 --
decode
```

L'cli-binary-formatoption est obligatoire si vous utilisez AWS CLI la version 2. Pour faire de ce paramètre le paramètre par défaut, exécutez `aws configure set cli-binary-format raw-in-base64-out`. Pour plus d'informations, consultez les options de ligne de commande globales AWS CLI prises en charge dans le Guide de l'utilisateur AWS Command Line Interface version 2.

Vous devriez voir la sortie suivante :

```
START RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8 Version: $LATEST
"AWS_SESSION_TOKEN": "AgoJb3JpZ2luX2VjELj...", "_X_AMZN_TRACE_ID": "Root=1-5d02e5ca-
f5792818b6fe8368e5b51d50;Parent=191db58857df8395;Sampled=0"",ask/lib:/opt/lib",
END RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8
REPORT RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8  Duration: 79.67 ms      Billed
 Duration: 80 ms         Memory Size: 128 MB     Max Memory Used: 73 MB
```

L'utilitaire `base64` est disponible sous Linux, macOS et Ubuntu sous Windows. Les utilisateurs de macOS auront peut-être besoin d'utiliser `base64 -D`.

Example Script get-logs.sh

Dans la même invite de commandes, utilisez le script suivant pour télécharger les cinq derniers événements de journalisation. Le script utilise `sed` pour supprimer les guillemets du fichier de sortie et attend 15 secondes pour permettre la mise à disposition des journaux. La sortie comprend la réponse de Lambda, ainsi que la sortie de la commande `get-log-events`.

Copiez le contenu de l'exemple de code suivant et enregistrez-le dans votre répertoire de projet Lambda sous `get-logs.sh`.

L'cli-binary-formatoption est obligatoire si vous utilisez AWS CLI la version 2. Pour faire de ce paramètre le paramètre par défaut, exécutez `aws configure set cli-binary-format raw-in-base64-out`. Pour plus d'informations, consultez les options de ligne de commande globales AWS CLI prises en charge dans le Guide de l'utilisateur AWS Command Line Interface version 2.

```
#!/bin/bash
aws lambda invoke --function-name my-function --cli-binary-format raw-in-base64-out --
payload '{"key": "value"}' out
sed -i'' -e 's/"//g' out
sleep 15
aws logs get-log-events --log-group-name /aws/lambda/my-function --log-stream-
name stream1 --limit 5
```

Example macOS et Linux (uniquement)

Dans la même invite de commande, les utilisateurs de macOS et de Linux devront peut-être exécuter la commande suivante pour s'assurer que le script est exécutable.

```
chmod -R 755 get-logs.sh
```

Example récupérer les cinq derniers événements de journal

Dans la même invite de commande, exécutez le script suivant pour obtenir les cinq derniers événements de journalisation.

```
./get-logs.sh
```

Vous devriez voir la sortie suivante:

```
{
    "StatusCode": 200,
    "ExecutedVersion": "$LATEST"
}
{
    "events": [
        {
            "timestamp": 1559763003171,
            "message": "START RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf Version:
 $LATEST\n",
            "ingestionTime": 1559763003309
        },
        {
            "timestamp": 1559763003173,
            "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tENVIRONMENT VARIABLES\r{\r  \"AWS_LAMBDA_FUNCTION_VERSION\": \"$LATEST\",
\r ...",
            "ingestionTime": 1559763018353
        },
        {
            "timestamp": 1559763003173,
            "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tEVENT\r{\r  \"key\": \"value\"\r}\n",
            "ingestionTime": 1559763018353
        },
        {
```

```
            "timestamp": 1559763003218,
            "message": "END RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf\n",
            "ingestionTime": 1559763018353
        },
        {
            "timestamp": 1559763003218,
            "message": "REPORT RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tDuration: 26.73 ms\tBilled Duration: 27 ms \tMemory Size: 128 MB\tMax Memory Used: 75
 MB\t\n",
            "ingestionTime": 1559763018353
        }
    ],
    "nextForwardToken": "f/34783877304859518393868359594929986069206639495374241795",
    "nextBackwardToken": "b/34783877303811383369537420289090800615709599058929582080"
}
```


Suppression de journaux

Les groupes de journaux ne sont pas supprimés automatiquement quand vous supprimez une fonction. Pour éviter de stocker des journaux indéfiniment, supprimez le groupe de journaux ou configurez une période de conservation à l'issue de laquelle les journaux sont supprimés automatiquement.

Instrumentation du Node.js code dans AWS Lambda

Lambda s'intègre pour vous aider AWS X-Ray à suivre, à déboguer et à optimiser les applications Lambda. Vous pouvez l'utiliser X-Ray pour suivre une demande lorsqu'elle parcourt les ressources de votre application, ce qui peut inclure des fonctions Lambda et AWS d'autres services.

Pour envoyer des données de suivi à X-Ray, vous pouvez utiliser l'une des deux bibliothèques du SDK :

- AWS Distro for OpenTelemetry (ADOT) — Une distribution sécurisée, prête pour la production et prise AWS en charge du SDK (OTel). OpenTelemetry
- Kit SDK AWS X-Ray pour Node.js— Un SDK pour générer et envoyer des données de trace à X-Ray.

Chacun des SDK propose des moyens d'envoyer vos données de télémétrie au service. X-Ray Vous pouvez ensuite les utiliser X-Ray pour afficher, filtrer et obtenir des informations sur les indicateurs de performance de votre application afin d'identifier les problèmes et les opportunités d'optimisation.

> **Important**
>
> Les X-Ray et Powertools for AWS Lambda SDK font partie d'une solution d'instrumentation étroitement intégrée proposée par. AWS Les couches ADOT Lambda font partie d'une norme industrielle pour l'instrumentation de traçage qui collecte plus de données en général, mais qui peut ne pas convenir à tous les cas d'utilisation. Vous pouvez implémenter le suivi de bout en bout à l' X-Ray aide de l'une ou l'autre solution. Pour en savoir plus sur le choix entre les deux, voir Choisir entre la AWS distribution pour Open Telemetry et les SDK. X-Ray

Sections

- Utiliser ADOT pour instrumenter vos fonctions Node.js
- Utiliser le X-Ray SDK pour instrumenter vos fonctions Node.js
- Activation du suivi avec la console Lambda
- Activation du suivi avec l'API Lambda
- Activation du traçage avec CloudFormation
- Interprétation et X-Ray traçage
- Stockage des dépendances d'exécution dans une couche (X-Ray SDK)

Utiliser ADOT pour instrumenter vos fonctions Node.js

ADOT fournit des couches Lambda entièrement gérées qui regroupent tout ce dont vous avez besoin pour collecter des données de télémétrie à l'aide du kit SDK OTel. En consommant cette couche, vous pouvez instrumenter vos fonctions Lambda sans avoir à modifier le code de fonction. Vous pouvez également configurer votre couche pour effectuer une initialisation personnalisée d'OTel. Pour de plus amples informations, veuillez consulter Configuration personnalisée pour ADOT Collector sur Lambda dans la documentation ADOT.

Pour les Node.js environnements d'exécution, vous pouvez ajouter la couche Lambda AWS gérée pour ADOT Javascript afin d'instrumenter automatiquement vos fonctions. Pour obtenir des instructions détaillées sur la façon d'ajouter cette couche, consultez AWS Distro for OpenTelemetry Lambda JavaScript Support dans la documentation ADOT.

Utiliser le X-Ray SDK pour instrumenter vos fonctions Node.js

Pour enregistrer les détails des appels que votre fonction d'événement Lambda effectue à d'autres ressources de votre application, vous pouvez également utiliser le. Kit SDK AWS X-Ray pour Node.js Pour obtenir ce kit SDK, ajoutez le package `aws-xray-sdk-core` aux dépendances de votre application.

Example vide- nodejs/package .json

```
{
  "name": "blank-nodejs",
  "version": "1.0.0",
  "private": true,
  "devDependencies": {
    "jest": "29.7.0"
  },
  "dependencies": {
    "@aws-sdk/client-lambda": "3.345.0",
    "aws-xray-sdk-core": "3.5.3"
  },
  "scripts": {
    "test": "jest"
  }
}
```

Pour instrumenter les clients du AWS SDK dans la AWS SDK pour JavaScript v3, encapsulez l'instance du client avec la `captureAWSv3Client` méthode.

Example vide- nodejs/function /index.js — Tracer un AWS Client du SDK

```
const AWSXRay = require('aws-xray-sdk-core');
const { LambdaClient, GetAccountSettingsCommand } = require('@aws-sdk/client-lambda');

// Create client outside of handler to reuse
const lambda = AWSXRay.captureAWSv3Client(new LambdaClient());

// Handler
exports.handler = async function(event, context) {
    event.Records.forEach(record => {
  ...
```

Le moteur d'exécution Lambda définit certaines variables d'environnement pour configurer le X-Ray SDK. Par exemple, Lambda définit sur pour éviter `AWS_XRAY_CONTEXT_MISSING` de `LOG_ERROR` générer des erreurs d'exécution depuis le X-Ray SDK. Pour définir une stratégie manquante de contexte personnalisée, remplacez la variable d'environnement dans votre configuration de fonction pour n'avoir aucune valeur, puis vous pouvez définir la stratégie manquante de contexte par programme.

Example Exemple de code d'initialisation

```
const AWSXRay = require('aws-xray-sdk-core');

// Configure the context missing strategy to do nothing
AWSXRay.setContextMissingStrategy(() => {});
```

Pour plus d’informations, consultez the section called “Variables d’environnement”.

Après avoir ajouté les bonnes dépendances et apporté les modifications de code nécessaires, activez le suivi dans la configuration de votre fonction via la console Lambda ou l'API.

Activation du suivi avec la console Lambda

Pour activer le suivi actif de votre fonction d'événement Lambda à l'aide de la console, procédez comme suit :

Pour activer le traçage actif

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez une fonction d'événement.

3. Choisissez Configuration, puis choisissez Outils de surveillance et d'opérations.
4. Dans Outils de surveillance supplémentaires, choisissez Modifier.
5. Sous Signaux CloudWatch d'application et AWS X-Ray sélectionnez Activer les traces de service Lambda.
6. Cliquez sur Enregistrer.

Activation du suivi avec l'API Lambda

Configurez le suivi sur votre fonction Lambda avec le AWS SDK AWS CLI or, utilisez les opérations d'API suivantes :

- UpdateFunctionConfiguration
- GetFunctionConfiguration
- CreateFunction

L'exemple de AWS CLI commande suivant active le suivi actif sur une fonction nommée my-function.

```
aws lambda update-function-configuration --function-name my-function \
--tracing-config Mode=Active
```

Le mode de suivi fait partie de la configuration spécifique de la version lorsque vous publiez une version de votre fonction. Vous ne pouvez pas modifier le mode de suivi sur une version publiée.

Activation du traçage avec CloudFormation

Pour activer le suivi d'une `AWS::Lambda::Function` ressource dans un CloudFormation modèle, utilisez la `TracingConfig` propriété.

Example fonction-inline.yml — Configuration du suivi

```
Resources:
  function:
    Type: AWS::Lambda::Function
    Properties:
      TracingConfig:
        Mode: Active
      ...
```

Pour une `AWS::Serverless::Function` ressource AWS Serverless Application Model (AWS SAM), utilisez la `Tracing` propriété.

Example template.yml — Configuration du suivi

```
Resources:
  function:
    Type: AWS::Serverless::Function
    Properties:
      Tracing: Active
      ...
```

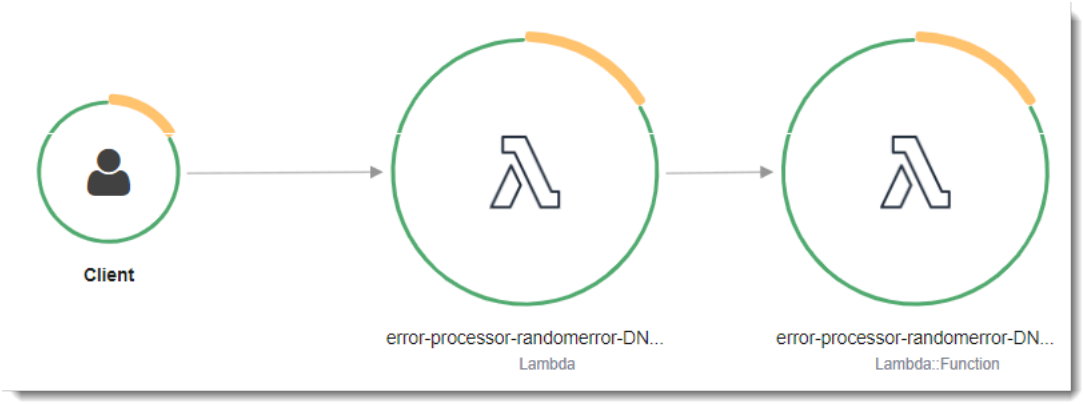
Interprétation et X-Ray traçage

Votre fonction événementielle a besoin d'une autorisation pour télécharger des données de suivi sur X-Ray. Lorsque vous activez le suivi dans la console Lambda, Lambda ajoute les autorisations requises au rôle d'exécution de votre fonction d'événement. Dans le cas contraire, ajoutez la AWSXRayDaemonWriteAccesspolitique au rôle d'exécution.

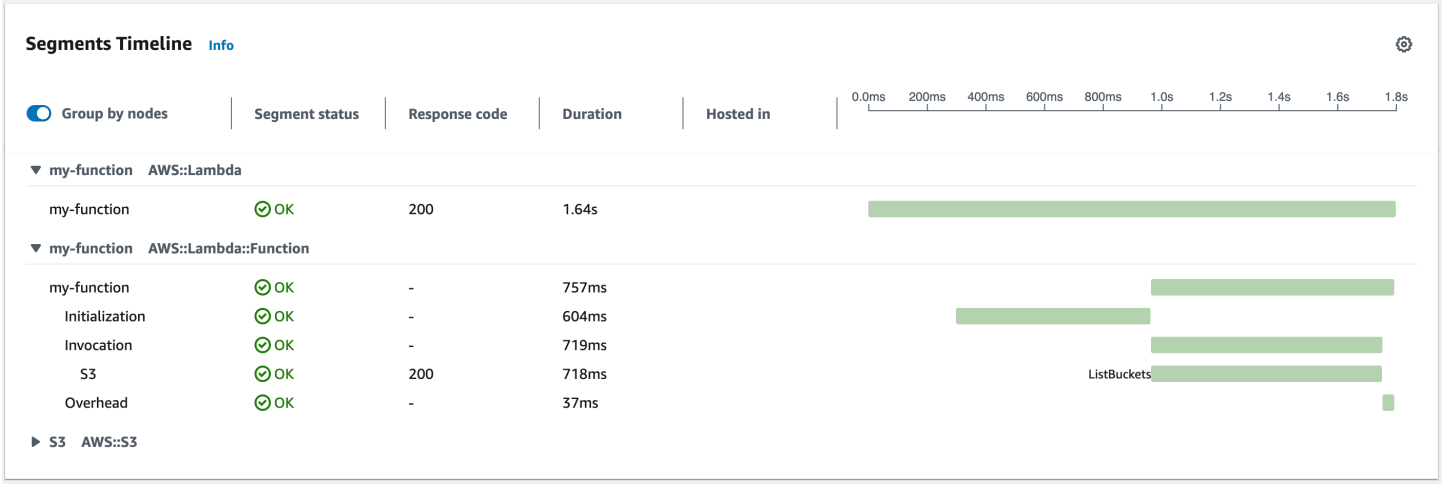
Une fois que vous avez configuré le suivi actif, vous pouvez observer des demandes spécifiques via votre application. Le graphique X-Ray de service affiche des informations sur votre application et tous ses composants. L'exemple suivant montre une application dotée de deux fonctions. La fonction principale traite les événements et renvoie parfois des erreurs. La deuxième fonction située en haut traite les erreurs qui apparaissent dans le groupe de journaux de la première et utilise le AWS SDK pour appeler X-Ray Amazon Simple Storage Service (Amazon S3) et Amazon Logs. CloudWatch

X-Ray n'assure pas le suivi de toutes les demandes jusqu'à votre application. X-Ray applique un algorithme d'échantillonnage pour garantir l'efficacité du suivi, tout en fournissant un échantillon représentatif de toutes les demandes. Le taux d'échantillonnage est 1 demande par seconde et 5 % de demandes supplémentaires. Vous ne pouvez pas configurer le taux X-Ray d'échantillonnage pour vos fonctions.

Dans X-Ray, un suivi enregistre des informations relatives à une demande traitée par un ou plusieurs services. Lambda enregistre deux segments par suivi, ce qui a pour effet de créer deux nœuds sur le graphique du service. L'image suivante met en évidence ces deux nœuds :



Le premier nœud sur la gauche représente le service Lambda qui reçoit la demande d'invocation. Le deuxième nœud représente votre fonction Lambda spécifique. L'exemple suivant illustre une trace avec ces deux segments. Les deux sont nommés my-function, mais l'un a pour origine `AWS::Lambda` et l'autre a pour origine `AWS::Lambda::Function`. Si le segment `AWS::Lambda` affiche une erreur, cela signifie que le service Lambda a rencontré un problème. Si le segment `AWS::Lambda::Function` affiche une erreur, cela signifie que votre fonction a rencontré un problème.



Cet exemple développe le segment `AWS::Lambda::Function` pour afficher ses trois sous-segments.

> **Note**
>
> AWS met actuellement en œuvre des modifications du service Lambda. En raison de ces modifications, vous pouvez constater des différences mineures entre la structure et le contenu des messages du journal système et des segments de trace émis par les différentes fonctions d'événement Lambda de votre ordinateur. Compte AWS
> L'exemple de suivi présenté ici illustre le segment de fonction à l'ancienne. Les différences entre les segments à l'ancienne et de style moderne sont décrites dans les paragraphes suivants.
> Ces modifications seront mises en œuvre au cours des prochaines semaines, et toutes les fonctions, Régions AWS sauf en Chine et dans les GovCloud régions, seront transférées pour utiliser le nouveau format des messages de journal et des segments de trace.

Le segment de fonction à l'ancienne contient les sous-segments suivants :

- Initialization (Initialisation) : représente le temps passé à charger votre fonction et à exécuter le code d'initialisation. Ce sous-segment apparaît pour le premier événement traité par chaque instance de votre fonction.
- Invocation – Représente le temps passé à exécuter votre code de gestionnaire.
- Overhead (Travail supplémentaire) – Représente le temps que le fichier d'exécution Lambda passe à se préparer à gérer l'événement suivant.

Le segment de fonction de style moderne ne contient pas de sous-segment `Invocation`. À la place, les sous-segments du client sont directement rattachés au segment de fonction. Pour plus d'informations sur la structure des segments de fonction à l'ancienne et de style moderne, consultez the section called "Comprendre les X-Ray traces".

Vous pouvez également utiliser des clients HTTP, enregistrer des requêtes SQL et créer des sous-segments personnalisés avec des annotations et des métadonnées. Pour plus d'informations, consultez Kit SDK AWS X-Ray pour Node.js dans le AWS X-Ray Guide du développeur.

> **Tarification**
>
> Vous pouvez utiliser le X-Ray suivi gratuitement chaque mois jusqu'à une certaine limite dans le cadre du niveau AWS gratuit. Au-delà de ce seuil, les X-Ray frais de stockage et de récupération des traces sont facturés. Pour en savoir plus, consultez Pricing AWS X-Ray (Tarification).

Stockage des dépendances d'exécution dans une couche (X-Ray SDK)

Si vous utilisez le X-Ray SDK pour instrumenter le code de fonction des clients du AWS SDK, votre package de déploiement peut devenir assez volumineux. Pour éviter de télécharger les dépendances d'exécution chaque fois que vous mettez à jour le code de votre fonction, empaquetez le X-Ray SDK dans une couche Lambda.

L'exemple suivant montre une ressource `AWS::Serverless::LayerVersion` qui stocke le Kit SDK AWS X-Ray pour Node.js.

Example template.yml — Couche de dépendances

```
Resources:
  function:
    Type: AWS::Serverless::Function
    Properties:
      CodeUri: function/.
      Tracing: Active
      Layers:
        - !Ref libs
      ...
  libs:
    Type: AWS::Serverless::LayerVersion
    Properties:
      LayerName: blank-nodejs-lib
      Description: Dependencies for the blank sample app.
      ContentUri: lib/.
      CompatibleRuntimes:
        - nodejs24.x
```

Avec cette configuration, vous ne mettez à jour les fichiers de couche de bibliothèque que si vous modifiez vos dépendances d’exécution. Étant donné que le package de déploiement de la fonction contient uniquement votre code, cela peut contribuer à réduire les temps de chargement.

La création d'une couche pour les dépendances nécessite des modifications de construction pour générer l'archive de couches avant le déploiement. Pour un exemple fonctionnel, consultez l'exemple d'application blank-nodejs.

Création de fonctions événementielles Lambda avec TypeScript

Vous pouvez utiliser Node.js temps d'exécution à exécuter TypeScript code dans AWS Lambda Fonctions événementielles. Parce que Node.js ne court pas TypeScript code en mode natif, vous devez d'abord transpiler votre TypeScript code dans JavaScript. Ensuite, utilisez JavaScript fichiers pour déployer le code de votre fonction sur Lambda. Votre code s'exécute dans un environnement qui inclut AWS SDK pour JavaScript, avec les informations d'identification d'un Gestion des identités et des accès AWS rôle (IAM) que vous gérez. Pour en savoir plus sur les versions du SDK incluses dans le Node.js temps d'exécution, voir the section called “Runtime-included Versions du SDK”.

Pour plus d'informations sur le traçage TypeScript fonctions avec, voir the section called “Tracing”.

Lambda prend en charge les éléments suivants Node.js temps d'exécution.

Nom	Identifiant	Système d'exploitation	Date d'obsolescence	Créer la fonction de blocage	Mettre à jour la fonction de blocage
Node.js 26	`nodejs26.x`	Amazon Linux 2	Non planifié	Non planifié	Non planifié
Node.js 24	`nodejs24.x`	Amazon Linux 2	30 avril 2028	1 juin 2028	1 juillet 2028
Node.js 22	`nodejs22.x`	Amazon Linux 2	30 avril 2027	29 juillet 2027	31 août 2027

Rubriques

- Configuration d'un TypeScript environnement de développement
- Définitions de type pour Lambda
- Définissez le gestionnaire de fonctions d'événement Lambda dans TypeScript
- Déployez TypeScript du code transpilé dans Lambda avec des archives de fichiers .zip

- Déployez TypeScript du code transpilé dans Lambda avec des images de conteneur
- Utilisation de l'objet de contexte Lambda pour récupérer les informations de la fonction TypeScript d'événement
- Enregistrez et surveillez les fonctions des TypeScript événements Lambda
- TypeScript Code de suivi dans AWS Lambda

Configuration d'un TypeScript environnement de développement

Utilisez un environnement de développement intégré (IDE) local ou un éditeur de texte pour rédiger votre TypeScript code de fonction. Vous ne pouvez pas créer TypeScript code sur la console Lambda.

Vous pouvez utiliser soit esbuild ou celui de Microsoft TypeScript compilateur (`tsc`) pour transpiler votre TypeScript code dans JavaScript. AWS Serverless Application Model (AWS SAM) et Cloud Development Kit AWS (AWS CDK) utilisent tous deux esbuild.

Tenez compte des éléments suivants lorsque vous utilisez esbuild :

- Il existe plusieurs TypeScript avertissements.
- Vous devez configurer votre TypeScript paramètres de transpilation pour correspondre à Node.js environnement d'exécution que vous prévoyez d'utiliser. Pour plus d'informations, consultez Cible dans la documentation d'esbuild. Pour un exemple de tsconfig.json fichier qui montre comment cibler une cible spécifique Node.js version prise en charge par Lambda, reportez-vous au TypeScript GitHub référentiel.
- esbuild n'effectue pas de vérifications de type. Pour vérifier les types, utilisez le compilateur `tsc`. Exécutez `tsc -noEmit` ou ajoutez un paramètre `"noEmit"` dans votre fichier tsconfig.json comme illustré dans l'exemple suivant. Cela configure `tsc` pour ne pas émettre JavaScript fichiers. Après avoir vérifié les types, utilisez esbuild pour convertir TypeScript fichiers dans JavaScript.

Example tsconfig.json

```
{
 "compilerOptions": {
   "target": "es2020",
   "strict": true,
   "preserveConstEnums": true,
   "noEmit": true,
```

```
    "sourceMap": false,
    "module":"commonjs",
    "moduleResolution":"node",
    "esModuleInterop": true,
    "skipLibCheck": true,
    "forceConsistentCasingInFileNames": true,
    "isolatedModules": true,
  },
  "exclude": ["node_modules", "**/*.test.ts"]
}
```

Définitions de type pour Lambda

Le @types/aws-lambda Le package fournit des définitions de type pour les fonctions événementielles Lambda. Installez ce package lorsque votre fonction utilise l'un des éléments suivants :

- Commun AWS sources d'événements, telles que :
  - `APIGatewayProxyEvent` : pour les intégrations de proxy Amazon API Gateway
  - `SNSEvent` : pour les notifications Amazon Simple Notification Service
  - `SQSEvent` : pour les messages Amazon Simple Queue Service
  - `S3Event` : pour les événements de déclencheur S3
  - `DynamoDBStreamEvent` : pour Amazon DynamoDB Streams
- L'objet Contexte Lambda
- Le modèle du gestionnaire de rappels

Pour ajouter les définitions de type Lambda à votre fonction, installez `@types/aws-lambda` en tant que dépendance de développement :

```
npm install -D @types/aws-lambda
```

Importez ensuite les types depuis `aws-lambda` :

```
import { Context, S3Event, APIGatewayProxyEvent } from 'aws-lambda';

export const handler = async (event: S3Event, context: Context) => {
    // Function code
};
```

L'instruction `import ... from 'aws-lambda'` importe les définitions de type. Elle n'importe pas le package npm `aws-lambda`, qui est un outil tiers indépendant. Pour plus d'informations, voir aws-lambda dans le DefinitelyTyped GitHub référentiel.

> **Note**
>
> Vous n'avez pas besoin @types/aws-lambda lorsque vous utilisez vos propres définitions de type personnalisées. Pour un exemple de fonction qui définit son propre type pour un objet d'événement, consultez Exemple de code de fonction d'événement TypeScript Lambda.

Définissez le gestionnaire de fonctions d'événement Lambda dans TypeScript

Le gestionnaire de fonctions d'événement Lambda est la méthode de votre code de fonction qui traite les événements. Lorsque votre fonction est invoquée, Lambda exécute la méthode du gestionnaire. Votre fonction s'exécute jusqu'à ce que le gestionnaire renvoie une réponse, se ferme ou expire.

Cette page explique comment utiliser les gestionnaires de fonctions d'événement Lambda dans TypeScript, notamment les options de configuration du projet, les conventions de dénomination et les meilleures pratiques. Cette page inclut également un exemple de fonction TypeScript Lambda qui collecte des informations relatives à une commande, produit un reçu sous forme de fichier texte et place ce fichier dans un bucket Amazon Simple Storage Service (Amazon S3). Pour plus d'informations sur le déploiement de votre fonction après l'avoir écrite, consultez the section called "Déployez des archives de fichiers .zip" ou the section called "Déploiement d'images de conteneur".

Rubriques

- Configuration de votre TypeScript projet
- Exemple de code de fonction d'événement TypeScript Lambda
- Modules CommonJS et ES
- Node.js initialisation
- Convention de nommage du gestionnaire
- Définition et accès à l'objet d'événement d'entrée
- Modèles de gestionnaire valides pour les fonctions TypeScript
- Utilisation du SDK pour la JavaScript version 3 dans votre gestionnaire
- Accès aux variables d'environnement
- Utilisation de l'état global
- Meilleures pratiques en matière de code pour les TypeScript fonctions d'événement Lambda

Configuration de votre TypeScript projet

Utilisez un environnement de développement intégré (IDE) local ou un éditeur de texte pour écrire votre code de TypeScript fonction. Vous ne pouvez pas créer de TypeScript code sur la console Lambda.

Il existe plusieurs manières d'initialiser un projet TypeScript Lambda. Par exemple, vous pouvez créer un projet en utilisant `npm`, créer une application AWS SAM ou créer une application AWS CDK. Pour créer un projet avec `npm` :

```
npm init
```

Le code de votre fonction se trouve dans un `.ts` fichier que vous transpirez dans un JavaScript fichier au moment de la création. Vous pouvez utiliser esbuild ou le TypeScript compilateur (`tsc`) de Microsoft pour transpiler votre TypeScript code dans. JavaScript Pour utiliser esbuild, ajoutez-le en tant que dépendance de développement :

```
npm install -D esbuild
```

Un projet de fonction TypeScript Lambda typique suit cette structure générale :

```
/project-root
  ### index.ts - Contains main handler
  ### dist/ - Contains compiled JavaScript
  ### package.json - Project metadata and dependencies
  ### package-lock.json - Dependency lock file
  ### tsconfig.json - TypeScript configuration
  ### node_modules/ - Installed dependencies
```

Exemple de code de fonction d'événement TypeScript Lambda

L'exemple de code de fonction Lambda suivant prend en compte les informations relatives à une commande, produit un reçu sous forme de fichier texte et place ce fichier dans un compartiment Amazon S3. Cet exemple définit un type d'événement personnalisé (`OrderEvent`). Pour savoir comment importer des définitions de type pour les sources d' AWS événements, consultez la section Définitions de type pour Lambda.

> **Note**
>
> Cet exemple utilise un gestionnaire de modules ES. Lambda prend en charge à la fois le module ES et les gestionnaires CommonJS. Pour plus d'informations, consultez Modules CommonJS et ES.

Example Fonction d'événement Lambda index.ts

```
import { S3Client, PutObjectCommand } from '@aws-sdk/client-s3';

// Initialize the S3 client outside the handler for reuse
const s3Client = new S3Client();
```

```
// Define the shape of the input event
type OrderEvent = {
    order_id: string;
    amount: number;
    item: string;
}

/**
 * Lambda handler for processing orders and storing receipts in S3.
 */
export const handler = async (event: OrderEvent): Promise<string> => {
    try {
        // Access environment variables
        const bucketName = process.env.RECEIPT_BUCKET;
        if (!bucketName) {
            throw new Error('RECEIPT_BUCKET environment variable is not set');
        }

        // Create the receipt content and key destination
        const receiptContent = `OrderID: ${event.order_id}\nAmount: $
${event.amount.toFixed(2)}\nItem: ${event.item}`;
        const key = `receipts/${event.order_id}.txt`;

        // Upload the receipt to S3
        await uploadReceiptToS3(bucketName, key, receiptContent);

        console.log(`Successfully processed order ${event.order_id} and stored receipt
 in S3 bucket ${bucketName}`);
        return 'Success';
    } catch (error) {
        console.error(`Failed to process order: ${error instanceof Error ?
 error.message : 'Unknown error'}`);
        throw error;
    }
};

/**
 * Helper function to upload receipt to S3
 */
async function uploadReceiptToS3(bucketName: string, key: string, receiptContent:
 string): Promise<void> {
    try {
        const command = new PutObjectCommand({
```

```
            Bucket: bucketName,
            Key: key,
            Body: receiptContent
        });

        await s3Client.send(command);
    } catch (error) {
        throw new Error(`Failed to upload receipt to S3: ${error instanceof Error ?
 error.message : 'Unknown error'}`);
    }
}
```

Ce fichier `index.ts` comprend les sections suivantes :

- Bloc `import` : utilisez ce bloc pour inclure les bibliothèques que votre fonction Lambda requiert, comme les clients du SDK AWS.
- Déclaration `const s3Client` : initialise un client Amazon S3 en dehors de la fonction du gestionnaire. Lambda exécute donc ce code pendant la phase d'initialisation, et le client est conservé pour être réutilisé lors de plusieurs appels.
- `type OrderEvent` : définit la structure de l'événement d'entrée attendu.
- `export const handler` : le gestionnaire de la fonction principal que Lambda invoque. Lorsque vous déployez votre fonction, spécifiez `index.handler` pour la propriété Gestionnaire. La valeur de la propriété `Handler` est le nom du fichier et le nom de la méthode du gestionnaire exporté, séparés par un point.
- Fonction `uploadReceiptToS3` : une fonction d'assistance référencée par la fonction du gestionnaire principal.

Pour que cette fonction fonctionne correctement, son rôle d'exécution doit autoriser l'action `s3:PutObject`. Assurez-vous également de définir la variable d'environnement `RECEIPT_BUCKET`. Après une invocation réussie, le compartiment Amazon S3 doit contenir un fichier de reçu.

Modules CommonJS et ES

Node.js prend en charge deux systèmes de modules : les modules CommonJS et ECMAScript (modules ES). Lambda recommande d'utiliser les modules ES car ils prennent en charge l'attente de haut niveau, ce qui permet d'effectuer des tâches asynchrones lors de l'initialisation de l'environnement d'exécution.

Node.js traite les fichiers avec une extension de nom de `.cjs` fichier comme des modules CommonJS tandis qu'une `.mjs` extension désigne les modules ES. Par défaut, Node.js traite les fichiers portant l'extension de nom de `.js` fichier comme des modules CommonJS. Vous pouvez configurer Node.js pour traiter les `.js` fichiers comme des modules ES en spécifiant le `type` as `module` dans le `package.json` fichier de la fonction. Vous pouvez configurer Node.js Lambda pour détecter automatiquement si un `.js` fichier doit être traité comme CommonJS ou comme un module ES en ajoutant l'`–experimental-detect-module`indicateur à la `NODE_OPTIONS` variable d'environnement. Pour plus d'informations, consultez la section Node.js Fonctionnalités expérimentales.

Les exemples suivants montrent des gestionnaires de fonctions écrits à l'aide de modules ES et de modules CommonJS. Les autres exemples de cette page utilisent tous des modules ES.

Node.js initialisation

Node.js utilise un I/O modèle non bloquant qui prend en charge des opérations asynchrones efficaces à l'aide d'une boucle d'événements. Par exemple, si elle Node.js effectue un appel réseau, la fonction continue de traiter les autres opérations sans bloquer la réponse du réseau. Lorsque la réponse du réseau est reçue, elle est placée dans la file de rappel. Les tâches de la file d'attente sont traitées lorsque la tâche en cours est terminée.

Lambda recommande d'utiliser l'attente de haut niveau afin que les tâches asynchrones initiées lors de l'initialisation de l'environnement d'exécution soient terminées pendant l'initialisation. Les tâches asynchrones qui ne sont pas terminées lors de l'initialisation sont généralement exécutées lors de la première invocation de la fonction. Cela peut entraîner un comportement inattendu ou des erreurs.

Par exemple, l'initialisation de votre fonction peut effectuer un appel réseau pour récupérer un paramètre depuis le Parameter Store AWS . Si cette tâche n'est pas terminée lors de l'initialisation, la valeur peut être nulle lors d'un appel. Il peut également y avoir un délai entre l'initialisation et l'appel, ce qui peut déclencher des erreurs lors d'opérations sensibles au facteur temps. En particulier, les appels de AWS service peuvent s'appuyer sur des signatures de demande urgentes, ce qui entraîne l'échec des appels de service si l'appel n'est pas terminé pendant la phase d'initialisation.

L'exécution des tâches lors de l'initialisation améliore généralement les performances de démarrage à froid et les performances d'appel d'abord lors de l'utilisation de la concurrence provisionnée. Pour plus d'informations, consultez notre article de blog Using Node.js ES modules and top-level await in AWS Lambda.

Convention de nommage du gestionnaire

Lorsque vous configurez une fonction, la valeur du paramètre Gestionnaire est le nom du fichier et le nom de la méthode du gestionnaire exporté, séparés par un point. La valeur par défaut des fonctions créées dans la console et dans les exemples de ce guide est `index.handler`. Cela indique la méthode `handler` qui est exportée à partir du fichier `index.js` ou `index.mjs`.

Si vous créez une fonction dans la console en utilisant un nom de fichier ou un nom de gestionnaire de fonction différent, vous devez modifier le nom du gestionnaire par défaut.

Pour modifier le nom du gestionnaire de fonction (console)

1. Ouvrez la page Fonctions de la console Lambda et choisissez votre fonction.
2. Cliquez sur l'onglet Code.
3. Faites défiler l'écran jusqu'au volet Paramètres d'exécution et choisissez Modifier.
4. Dans Gestionnaire, saisissez le nouveau nom de votre gestionnaire de fonction.
5. Cliquez sur Enregistrer.

Définition et accès à l'objet d'événement d'entrée

JSON est le format d'entrée le plus courant et le plus standard pour les fonctions d'événement Lambda. Dans cet exemple, la fonction exige une entrée similaire à l'exemple suivant :

```
{
    "order_id": "12345",
    "amount": 199.99,
    "item": "Wireless Headphones"
}
```

Lorsque vous utilisez des fonctions Lambda dans TypeScript, vous pouvez définir la forme de l'événement d'entrée à l'aide d'un type ou d'une interface. Dans cet exemple, nous définissons la structure de l'événement à l'aide d'un type :

```
type OrderEvent = {
    order_id: string;
    amount: number;
    item: string;
}
```

Après avoir défini le type ou l'interface, utilisez-le dans la signature de votre gestionnaire pour garantir la sécurité du type :

```
export const handler = async (event: OrderEvent): Promise<string> => {
```

Lors de la compilation, TypeScript vérifie que l'objet d'événement contient les champs obligatoires avec les types corrects. Par exemple, le TypeScript compilateur signale une erreur si vous essayez de l'utiliser `event.order_id` sous forme de nombre ou `event.amount` de chaîne.

Modèles de gestionnaire valides pour les fonctions TypeScript

Nous vous recommandons de async/awaitdéclarer le gestionnaire de fonctions au lieu d'utiliser des rappels. Async/await est un moyen concis et lisible d'écrire du code asynchrone, sans avoir besoin de rappels imbriqués ou de promesses enchaînées. Avec async/await, vous pouvez écrire du code qui se lit comme du code synchrone, tout en étant asynchrone et non bloquant.

Les exemples de cette section utilisent le type `S3Event`. Vous pouvez toutefois utiliser n'importe quel autre type d' AWS événement dans le package @ types/aws -lambda ou définir votre propre type d'événement. Pour utiliser des types provenant de @types/aws-lambda :

1. Ajoutez le package @types/aws-lambda en tant que dépendance de développement :

   ```
   npm install -D @types/aws-lambda
   ```

2. Importez les types dont vous avez besoin, comme `Context`, `S3Event` ou `Callback`.

gestionnaires de fonctions asynchrones (recommandé)

Le mot-clé `async` marque une fonction comme étant asynchrone, et le mot-clé `await` met en pause l'exécution de la fonction jusqu'à ce qu'une `Promise` soit résolue. Le gestionnaire accepte les arguments suivants :

- `event` : contient les données d'entrée transmises à votre fonction.
- `context` : contient des informations sur l'invocation, la fonction et l'environnement d'exécution. Pour plus d'informations, consultez Utilisation de l'objet de contexte Lambda pour récupérer les informations de la fonction TypeScript d'événement.

Voici les signatures valides pour le async/await modèle :

```
export const handler = async (event: S3Event): Promise<void> => { };
```

```
export const handler = async (event: S3Event, context: Context): Promise<void> => { };
```

> **Note**
>
> Lorsque vous traitez des tableaux d'éléments de manière asynchrone, assurez-vous d'utiliser await avec `Promise.all` pour vous assurer que toutes les opérations sont terminées. Des méthodes comme `forEach` n'attendent pas la fin des rappels asynchrones. Pour plus d'informations, consultez Array.prototype.forEach() dans la documentation de Mozilla.

Gestionnaires de fonctions synchrones

Lorsque votre fonction n'exécute aucune tâche asynchrone, vous pouvez utiliser un gestionnaire de fonctions synchrones en utilisant l'une des signatures de fonction suivantes :

```
export const handler = (event: S3Event): void => { };
```

```
export const handler = (event: S3Event, context: Context): void => { };
```

Gestionnaires de fonctions de diffusion des réponses

Lambda prend en charge le streaming de réponses avec. Node.js Les gestionnaires de fonctions de streaming de réponses utilisent le décorateur AWSLambda.streamifyResponse () et prennent 3 paramètres : event, responseStream et context. La signature de la fonction est la suivante :

```
export const handler = awslambda.streamifyResponse(async (event: APIGatewayProxyEvent,
 responseStream: NodeJS.WritableStream, context: Context) => { });
```

Pour plus d'informations, consultez Streaming de réponses pour les fonctions Lambda.

Callback-based gestionnaires de fonctions

> **Note**
>
> Callback-based les gestionnaires de fonctions ne sont pris en charge que jusqu'à Node.js 22. À partir de Node.js 24, les tâches asynchrones doivent être implémentées à l'aide de gestionnaires de fonctions asynchrones.

Callback-based les gestionnaires de fonctions peuvent utiliser les arguments d'événement, de contexte et de rappel. L'argument de rappel attend une réponse `Error` et une réponse, qui doit être JSON-serializable.

Voici la signature valide pour le modèle de gestionnaire de rappel :

```
export const handler = (event: S3Event, context: Context, callback: Callback<void>):
 void => { };
```

La fonction continue à s'exécuter jusqu'à ce que la boucle d'événement soit vide ou que la fonction s'arrête. La réponse n'est pas envoyée à l'appelant tant que toutes les tâches d'événement de boucle ne sont pas terminées. Si la fonction expire, une erreur est renvoyée à la place. Vous pouvez configurer le moteur d'exécution pour envoyer la réponse immédiatement en attribuant à context.callback WaitsForEmptyEventLoop la valeur false.

Example TypeScript fonction avec rappel

L'exemple suivant utilise `APIGatewayProxyCallback`, un type de rappel spécialisé spécifique aux intégrations API Gateway. La plupart des sources d' AWS événements utilisent le `Callback` type générique indiqué dans les signatures ci-dessus.

```
import { Context, APIGatewayProxyCallback, APIGatewayEvent } from 'aws-lambda';

export const lambdaHandler = (event: APIGatewayEvent, context: Context, callback:
 APIGatewayProxyCallback): void => {
    console.log(`Event: ${JSON.stringify(event, null, 2)}`);
    console.log(`Context: ${JSON.stringify(context, null, 2)}`);
    callback(null, {
        statusCode: 200,
        body: JSON.stringify({
            message: 'hello world',
```

```
        }),
    });
};
```

Utilisation du SDK pour la JavaScript version 3 dans votre gestionnaire

Vous utiliserez souvent les fonctions Lambda pour interagir avec d'autres AWS ressources ou pour les mettre à jour. Le moyen le plus simple d'interagir avec ces ressources est d'utiliser AWS SDK pour JavaScript. Tous les environnements d' Node.js exécution Lambda pris en charge incluent le SDK pour la version 3. JavaScript Toutefois, nous vous recommandons vivement d'inclure les clients AWS SDK dont vous avez besoin dans votre package de déploiement. Cela permet d'optimiser la rétrocompatibilité lors des futures mises à jour de l'environnement d'exécution Lambda.

Pour ajouter des dépendances au SDK à votre fonction, utilisez la commande `npm install` correspondant aux clients SDK spécifiques dont vous avez besoin. Dans l'exemple de code, nous avons utilisé le client Amazon S3. Ajoutez cette dépendance en exécutant la commande suivante dans le répertoire qui contient votre fichier `package.json` :

```
npm install @aws-sdk/client-s3
```

Dans le code de fonction, importez le client et les commandes dont vous avez besoin, comme le montre l'exemple de fonction :

```
import { S3Client, PutObjectCommand } from '@aws-sdk/client-s3';
```

Initialisez ensuite un client Amazon S3 :

```
const s3Client = new S3Client();
```

Dans cet exemple, nous avons initialisé notre client Amazon S3 en dehors de la fonction de gestionnaire principale pour éviter d'avoir à l'initialiser à chaque fois que nous invoquons notre fonction. Après avoir initialisé votre client SDK, vous pouvez l'utiliser pour effectuer des appels d'API pour ce AWS service. L'exemple de code appelle l'action d'PutObjectAPI Amazon S3 comme suit :

```
const command = new PutObjectCommand({
    Bucket: bucketName,
    Key: key,
    Body: receiptContent
```

```
});
```

Accès aux variables d'environnement

Dans le code de votre gestionnaire, vous pouvez référencer n'importe quelle variable d'environnement à l'aide de `process.env`. Dans cet exemple, nous référençons la variable d'environnement `RECEIPT_BUCKET` définie à l'aide des lignes de code suivantes :

```
// Access environment variables
const bucketName = process.env.RECEIPT_BUCKET;
if (!bucketName) {
    throw new Error('RECEIPT_BUCKET environment variable is not set');
}
```

Utilisation de l'état global

Lambda exécute votre code statique pendant la phase d'initialisation avant d'invoquer votre fonction pour la première fois. Les ressources créées pendant l'initialisation restent en mémoire entre les invocations, ce qui vous évite d'avoir à les créer chaque fois que vous invoquez votre fonction.

Dans l'exemple de code, le code d'initialisation du client S3 se trouve en dehors du gestionnaire. L'exécution initialise le client avant que la fonction n'exécute son premier événement, et le client reste disponible pour être réutilisé pendant toutes les invocations.

Meilleures pratiques en matière de code pour les TypeScript fonctions d'événement Lambda

Suivez ces instructions pour créer des fonctions Lambda :

- Séparez le gestionnaire Lambda de votre logique principale. Cela vous permet de créer une fonction testable plus unitaire.
- Contrôlez les dépendances du package de déploiement de vos fonctions. L'environnement AWS Lambda d'exécution contient un certain nombre de bibliothèques. Pour les Node.js environnements d'exécution et Python, ceux-ci incluent les AWS SDK. Pour activer le dernier ensemble de mises à jour des fonctionnalités et de la sécurité, Lambda met régulièrement à jour ces bibliothèques. Ces mises à jour peuvent introduire de subtiles modifications dans le comportement de votre fonction Lambda. Pour disposer du contrôle total des dépendances que votre fonction utilise, empaquetez toutes vos dépendances avec votre package de déploiement.
- Réduisez la complexité de vos dépendances. Privilégiez les infrastructures plus simples qui se chargent rapidement au démarrage de l'environnement d'exécution.

- Réduisez la taille de votre package de déploiement selon ses besoins d'exécution. Cela contribue à réduire le temps nécessaire au téléchargement et à la décompression de votre package de déploiement avant l'invocation.

Tirez parti de la réutilisation de l'environnement d'exécution pour améliorer les performances de votre fonction. Initialisez les clients SDK et les connexions à la base de données en dehors du gestionnaire de fonctions et mettez en cache les actifs statiques localement dans le répertoire `/tmp`. Les invocations ultérieures traitées par la même instance de votre fonction peuvent réutiliser ces ressources. Cela permet d'économiser des coûts, tout en réduisant le temps d'exécution de la fonction.

Pour éviter des éventuelles fuites de données entre les invocations, n'utilisez pas l'environnement d'exécution pour stocker des données utilisateur, des événements ou d'autres informations ayant un impact sur la sécurité. Si votre fonction repose sur un état réversible qui ne peut pas être stocké en mémoire dans le gestionnaire, envisagez de créer une fonction distincte ou des versions distinctes d'une fonction pour chaque utilisateur.

Utilisez une directive keep-alive pour maintenir les connexions persistantes. Lambda purge les connexions inactives au fil du temps. Si vous tentez de réutiliser une connexion inactive lorsque vous invoquez une fonction, cela entraîne une erreur de connexion. Pour maintenir votre connexion persistante, utilisez la directive Keep-alive associée à votre environnement d'exécution. Pour un exemple, voir Réutilisation des connexions avec Keep-Alive in Node.js.

Utilisez des variables d'environnement pour transmettre des paramètres opérationnels à votre fonction. Par exemple, si vous écrivez dans un compartiment Amazon S3 au lieu de coder en dur le nom du compartiment dans lequel vous écrivez, configurez le nom du compartiment comme variable d'environnement.

Évitez d'utiliser des invocations récursives dans votre fonction Lambda, lorsque la fonction s'invoque elle-même ou démarre un processus susceptible de l'invoquer à nouveau. Cela peut entraîner un volume involontaire d'invocations de fonction et des coûts accrus. Si vous constatez un volume involontaire d'invocations, définissez immédiatement la simultanéité réservée à la fonction sur `0` afin de limiter toutes les invocations de la fonction, pendant que vous mettez à jour le code.

N'utilisez pas d'API non publiques non documentées dans le code de votre fonction Lambda. Pour les AWS Lambda environnements d'exécution gérés, Lambda applique régulièrement des mises à jour fonctionnelles et de sécurité aux API internes de Lambda. Ces mises à jour internes de l'API peuvent être incompatibles avec les versions antérieures, entraînant des conséquences imprévues telles que

des échecs d'invocation si votre fonction dépend de ces API non publiques. Consultez la Référence d'API pour obtenir la liste des API accessibles au public.

Écriture du code idempotent. L'écriture de code idempotent pour vos fonctions garantit ne gestion identique des événements dupliqués. Votre code doit valider correctement les événements et gérer correctement les événements dupliqués. Pour de plus amples informations, veuillez consulterComment faire en sorte que ma fonction Lambda soit idempotente ?.

Déployez TypeScript du code transpilé dans Lambda avec des archives de fichiers .zip

Avant de pouvoir déployer TypeScript du code sur AWS Lambda, vous devez le transpiler dans JavaScript. Cette page explique trois méthodes pour créer et déployer TypeScript du code sur Lambda avec des archives de fichiers .zip :

- En utilisant AWS Serverless Application Model (AWS SAM)
- À l'aide du Cloud Development Kit AWS (AWS CDK)
- Utilisation de la AWS Command Line Interface (AWS CLI) et d'esbuild

AWS SAM et AWS CDK simplifiez la création et le déploiement TypeScript des fonctions. La spécification du modèle AWS SAM fournit une syntaxe simple et propre pour décrire les fonctions Lambda, les API, les autorisations, les configurations et les événements qui composent votre application sans serveur. Avec le AWS CDK, vous pouvez créer des applications fiables, évolutives et économiques dans le cloud avec la puissance expressive considérable d'un langage de programmation. AWS CDK Il est destiné aux AWS utilisateurs modérément à très expérimentés. Le AWS CDK et le AWS SAM utilisent esbuild pour transpiler le TypeScript code dans. JavaScript

Utilisation AWS SAM pour déployer TypeScript du code sur Lambda

Suivez les étapes ci-dessous pour télécharger, créer et déployer un exemple d' TypeScript application Hello World à l'aide du AWS SAM. Cette application implémente un backend API de base. Il se compose d'un point de terminaison Amazon API Gateway et d'une fonction d'événement Lambda. Lorsque vous envoyez une demande GET au point de terminaison API Gateway, la fonction Lambda est invoquée. La fonction renvoie un message `hello world`.

> **Note**
>
> AWS SAM utilise esbuild pour créer des fonctions Node.js Lambda à TypeScript partir du code. Le support d'esbuild est actuellement en version préliminaire publique. Lors de la préversion publique, le support d'esbuild peut être soumis à des modifications rétroincompatibles.

Conditions préalables

Pour exécuter la procédure indiquée dans cette section, vous devez satisfaire aux exigences suivantes :

- AWS CLI version 2
- AWS SAM CLI version 1.75 ou ultérieure
- Node.js

Déployer un échantillon AWS SAM vigie

1. Initialisez l'application à l'aide du TypeScript modèle Hello World.

```
sam init --app-template hello-world-typescript --name sam-app --package-type Zip --
runtime nodejs24.x
```

2. (Facultatif) L'exemple d'application inclut des configurations pour les outils couramment utilisés, tels que ESLlint pour la validation de code et de Jest pour les tests unitaires. Pour exécuter des commandes de test et de validation :

```
cd sam-app/hello-world
npm install
npm run lint
npm run test
```

3. Créez l'application.

```
cd sam-app
sam build
```

4. Déployez l'application.

```
sam deploy --guided
```

5. Suivez les invites à l'écran. Répondez avec `Enter` pour accepter les options par défaut fournies dans l'expérience interactive.
6. La sortie affiche le point de terminaison de l'API REST. Ouvrez le point de terminaison dans un navigateur pour tester la fonction. Vous devriez voir la réponse suivante :

```
{"message":"hello world"}
```

7. Il s'agit d'un point de terminaison d'API public accessible par Internet. Nous vous recommandons de supprimer le point de terminaison après un test.

```
sam delete
```

Utilisation de AWS CDK pour déployer TypeScript du code sur Lambda

Suivez les étapes ci-dessous pour créer et déployer un exemple d' TypeScript application à l'aide du AWS CDK. Cette application implémente un backend API de base. Elle se compose d'un point de terminaison API Gateway et d'une fonction Lambda. Lorsque vous envoyez une demande GET au point de terminaison API Gateway, la fonction Lambda est invoquée. La fonction renvoie un message `hello world`.

Conditions préalables

Pour exécuter la procédure indiquée dans cette section, vous devez satisfaire aux exigences suivantes :

- AWS CLI version 2
- AWS CDK version 2
- Node.js
- Docker ou esbuild

Déployer un échantillon AWS CDK vigie

1. Créez un répertoire de projets pour votre nouvelle application.

   ```
   mkdir hello-world
   cd hello-world
   ```

2. Initialisez l'application.

   ```
   cdk init app --language typescript
   ```

3. Ajoutez le package @ types/aws -lambda en tant que dépendance de développement. Ce package contient les définitions de type pour Lambda.

   ```
   npm install -D @types/aws-lambda
   ```

4. Ouvrez le répertoire lib. Vous devriez voir un fichier nommé hello-world-stack.ts. Créez deux nouveaux fichiers dans ce répertoire : hello-world.function.ts et hello-world.ts.

5. Ouvrez hello-world.function.ts et ajoutez le code suivant au fichier. Il s'agit du code de la fonction Lambda.

> **Note**
>
> L'`import`instruction importe les définitions de type depuis @ types/aws -lambda. Elle n'importe pas le package NPM `aws-lambda`, qui est un outil tiers indépendant. Pour plus d'informations, consultez aws-lambda dans le référentiel. DefinitelyTyped GitHub

```
import { Context, APIGatewayProxyResult, APIGatewayEvent } from 'aws-lambda';

export const handler = async (event: APIGatewayEvent, context: Context):
 Promise<APIGatewayProxyResult> => {
    console.log(`Event: ${JSON.stringify(event, null, 2)}`);
    console.log(`Context: ${JSON.stringify(context, null, 2)}`);
    return {
        statusCode: 200,
        body: JSON.stringify({
            message: 'hello world',
        }),
    };
};
```

6. Ouvrez hello-world.ts et ajoutez le code suivant au fichier. Il contient la NodejsFunction construction, qui crée la fonction Lambda, et la LambdaRestApi construction, qui crée l'API REST.

```
import { Construct } from 'constructs';
import { NodejsFunction } from 'aws-cdk-lib/aws-lambda-nodejs';
import { LambdaRestApi } from 'aws-cdk-lib/aws-apigateway';

export class HelloWorld extends Construct {
  constructor(scope: Construct, id: string) {
    super(scope, id);
    const helloFunction = new NodejsFunction(this, 'function');
    new LambdaRestApi(this, 'apigw', {
      handler: helloFunction,
    });
  }
}
```

Le composant `NodejsFunction` suppose les éléments suivants par défaut :

- Votre gestionnaire de fonctions se nomme `handler`.
- Le fichier .ts qui contient le code de fonction (hello-world.function.ts) se trouve dans le même répertoire que le fichier .ts qui contient le composant (hello-world.ts). Le composant utilise l'ID du composant (« hello-world ») et le nom du fichier du gestionnaire Lambda (« fonction ») pour trouver le code de la fonction. Par exemple, si le code de votre fonction se trouve dans un fichier nommé hello-world.my-fonction.ts, le fichier hello-world.ts doit référencer le code de la fonction comme suit :

```
const helloFunction = new NodejsFunction(this, 'my-function');
```

Vous pouvez modifier ce comportement et configurer d'autres paramètres esbuild. Pour plus d'informations, consultez Configuration d'esbuild dans la référence de l' AWS CDK API.

7. Ouvrez hello-world stack.ts. C'est le code qui définit votre pile de AWS CDK. Remplacez le code par ce qui suit :

```
import { Stack, StackProps } from 'aws-cdk-lib';
import { Construct } from 'constructs';
import { HelloWorld } from './hello-world';

export class HelloWorldStack extends Stack {
  constructor(scope: Construct, id: string, props?: StackProps) {
    super(scope, id, props);
    new HelloWorld(this, 'hello-world');
  }
}
```

8. à partir du répertoire `hello-world` contenant votre fichier `cdk.json`, déployez votre application.

```
cdk deploy
```

9. AWS CDK Construit et empaquète la fonction Lambda à l'aide d'esbuild, puis déploie la fonction dans le moteur d'exécution Lambda. La sortie affiche le point de terminaison de l'API REST. Ouvrez le point de terminaison dans un navigateur pour tester la fonction. Vous devriez voir la réponse suivante :

```
{"message":"hello world"}
```

Il s'agit d'un point de terminaison d'API public accessible par Internet. Nous vous recommandons de supprimer le point de terminaison après un test.

Utilisation de AWS CLI et esbuild pour déployer du TypeScript code sur Lambda

L'exemple suivant montre comment transpiler et déployer TypeScript du code sur Lambda à l'aide d'esbuild et de. esbuild produit JavaScript un fichier avec toutes AWS CLI les dépendances. Il s'agit du seul fichier que vous devez ajouter à l'archive .zip.

Conditions préalables

Pour exécuter la procédure indiquée dans cette section, vous devez satisfaire aux exigences suivantes :

- AWS CLI version 2
- Node.js
- Un rôle d'exécution pour votre fonction Lambda
- Pour les utilisateurs de Windows, un utilitaire de fichier zip tel que 7zip.

Déployez un exemple de fonction

1. Sur votre machine locale, créez un répertoire de projets pour votre nouvelle fonction.
2. Créez un nouveau Node.js projet avec npm ou un gestionnaire de packages de votre choix.

   ```
   npm init
   ```

3. Ajoutez les packages @ types/aws -lambda et esbuild en tant que dépendances de développement. Le package `@types/aws-lambda` contient les définitions de type pour Lambda.

   ```
   npm install -D @types/aws-lambda esbuild
   ```

4. Créez un nouveau fichier nommé index.ts. Ajoutez le code suivant au nouveau fichier. Il s'agit du code de la fonction Lambda. La fonction renvoie un message `hello world`. La fonction ne crée aucune ressource API Gateway.

> **Note**
>
> L'`import`instruction importe les définitions de type depuis @ types/aws -lambda. Elle n'importe pas le package NPM `aws-lambda`, qui est un outil tiers indépendant. Pour plus d'informations, consultez aws-lambda dans le référentiel. DefinitelyTyped GitHub

```
import { Context, APIGatewayProxyResult, APIGatewayEvent } from 'aws-lambda';

export const handler = async (event: APIGatewayEvent, context: Context):
 Promise<APIGatewayProxyResult> => {
  console.log(`Event: ${JSON.stringify(event, null, 2)}`);
  console.log(`Context: ${JSON.stringify(context, null, 2)}`);
  return {
      statusCode: 200,
      body: JSON.stringify({
          message: 'hello world',
      }),
   };
};
```

5. Ajoutez un script de génération au fichier package.json. Ceci permet de configurer esbuild pour créer automatiquement le pack de déploiement .zip. Pour plus d'informations, consultez Scripts de génération dans la documentation d'esbuild.

   Linux and MacOS

   ```
   "scripts": {
     "prebuild": "rm -rf dist",
     "build": "esbuild index.ts --bundle --minify --sourcemap --platform=node --
   target=es2020 --outfile=dist/index.js",
     "postbuild": "cd dist && zip -r index.zip index.js*"
   },
   ```

   Windows

   Dans cet exemple, la commande `"postbuild"` utilise l'utilitaire 7zip pour créer votre fichier .zip. Utilisez votre propre utilitaire Windows zip préféré et modifiez la commande si nécessaire.

```
"scripts": {
  "prebuild": "del /q dist",
  "build": "esbuild index.ts --bundle --minify --sourcemap --platform=node --
target=es2020 --outfile=dist/index.js",
  "postbuild": "cd dist && 7z a -tzip index.zip index.js*"
},
```

6. Créez le pack.

```
npm run build
```

7. Créez une fonction Lambda à l'aide du pack de déploiement .zip. Remplacez le texte surligné par l'Amazon Resource Name (ARN) de votre rôle d'exécution.

```
aws lambda create-function --function-name hello-world --runtime "nodejs24.x" --
role arn:aws:iam::123456789012:role/lambda-ex --zip-file "fileb://dist/index.zip"
 --handler index.handler
```

8. Exécutez un événement de test pour confirmer que la fonction renvoie la réponse suivante. Si vous souhaitez invoquez cette fonction à l'aide d'API Gateway, créez et configurez l'API REST.

```
{
  "statusCode": 200,
  "body": "{\"message\":\"hello world\"}"
}
```

Déployez TypeScript du code transpilé dans Lambda avec des images de conteneur

Vous pouvez déployer votre TypeScript code dans une fonction d' AWS Lambda événement sous forme d'image de Node.js conteneur. AWS fournit des images de base Node.js pour vous aider à créer l'image du conteneur. Ces images de base sont préchargées avec un environnement d'exécution du langage et d'autres composants nécessaires pour exécuter l'image sur Lambda. AWS fournit un Dockerfile pour chacune des images de base afin de vous aider à créer votre image de conteneur.

Si vous utilisez une image de base d'une communauté ou d'une entreprise privée, vous devez ajouter le client Node.js d'interface d'exécution (RIC) à l'image de base pour la rendre compatible avec Lambda.

Lambda fournit un émulateur d'interface d'exécution pour les tests locaux. Les images AWS de base Node.js incluent l'émulateur d'interface d'exécution. Si vous utilisez une autre image de base, telle qu'une image Alpine Linux ou Debian, vous pouvez intégrer l'émulateur dans votre image ou l'installer sur votre ordinateur local.

Utilisation d'une image Node.js de base pour créer et empaqueter le code de TypeScript fonction

Conditions préalables

Pour exécuter la procédure indiquée dans cette section, vous devez satisfaire aux exigences suivantes :

- AWS CLI version 2
- Docker (version minimale 25.0.0)
- Le plug-in buildx Docker.
- Node.js 22,x

Création d'une image à partir d'une image de base

Pour créer une image à partir d'un AWS image de base pour Lambda

1. Sur votre machine locale, créez un répertoire de projets pour votre nouvelle fonction.
2. Créez un nouveau Node.js projet `npm` ou un gestionnaire de packages de votre choix.

```
npm init
```

3. Ajoutez les packages @ types/aws -lambda et esbuild en tant que dépendances de développement. Le package `@types/aws-lambda` contient les définitions de type pour Lambda.

```
npm install -D @types/aws-lambda esbuild
```

4. Ajoutez un script de création au fichier `package.json`.

```
  "scripts": {
  "build": "esbuild index.ts --bundle --minify --sourcemap --platform=node --
target=es2020 --outfile=dist/index.js"
}
```

5. Créez un nouveau fichier appelé `index.ts`. Ajoutez l'exemple de code suivant au nouveau fichier. Il s'agit du code de la fonction Lambda. La fonction renvoie un message `hello world`.

> **Note**
>
> L'`import`instruction importe les définitions de type depuis @ types/aws -lambda. Elle n'importe pas le package NPM `aws-lambda`, qui est un outil tiers indépendant. Pour plus d'informations, consultez aws-lambda dans le référentiel. DefinitelyTyped GitHub

```
import { Context, APIGatewayProxyResult, APIGatewayEvent } from 'aws-lambda';

export const handler = async (event: APIGatewayEvent, context: Context):
 Promise<APIGatewayProxyResult> => {
    console.log(`Event: ${JSON.stringify(event, null, 2)}`);
    console.log(`Context: ${JSON.stringify(context, null, 2)}`);
    return {
        statusCode: 200,
        body: JSON.stringify({
            message: 'hello world',
        }),
    };
};
```

6. Créez un nouveau Dockerfile avec la configuration suivante :

   - Définissez la propriété `FROM` sur l'URI de l'image de base.

- Définissez l'argument `CMD` pour spécifier le gestionnaire de la fonction Lambda.

L'exemple de fichier Docker suivant utilise une génération en plusieurs étapes. La première étape consiste à transspirer le TypeScript code en. JavaScript La deuxième étape produit une image de conteneur contenant uniquement des JavaScript fichiers et des dépendances de production.

Notez que l'exemple de Dockerfile n'inclut pas d'instruction USER. Lorsque vous déployez une image de conteneur sur Lambda, Lambda définit automatiquement un utilisateur Linux par défaut disposant d'autorisations de moindre privilège. Ceci est différent du comportement standard de Docker qui est défini par défaut par l'utilisateur `root` lorsqu'aucune instruction USER n'est fournie.

Example Dockerfile

```
FROM public.ecr.aws/lambda/nodejs:22 as builder
WORKDIR /usr/app
COPY package.json index.ts  ./
RUN npm install
RUN npm run build

FROM public.ecr.aws/lambda/nodejs:22
WORKDIR ${LAMBDA_TASK_ROOT}
COPY --from=builder /usr/app/dist/* ./
CMD ["index.handler"]
```

7. Générez l'image Docker à l'aide de la commande docker build. L'exemple suivant nomme l'image `docker-image` et lui donne la balise `test`. Pour rendre votre image compatible avec Lambda, vous devez utiliser l'option `--provenance=false`.

```
docker buildx build --platform linux/amd64 --provenance=false -t docker-image:test
 .
```

> **Note**
>
> La commande spécifie l'option `--platform linux/amd64` pour garantir la compatibilité de votre conteneur avec l'environnement d'exécution Lambda, quelle que soit l'architecture de votre machine de génération. Si vous avez l'intention de créer une

fonction Lambda à l'aide de l'architecture du jeu d'instructions ARM64, veillez à modifier la commande pour utiliser plutôt l'option `--platform linux/arm64`.

(Facultatif) Testez l'image localement

1. Démarrez votre image Docker à l'aide de la commande docker run. Dans cet exemple, `docker-image` est le nom de l'image et `test` est la balise.

```
docker run --platform linux/amd64 -p 9000:8080 docker-image:test
```

Cette commande exécute l'image en tant que conteneur et crée un point de terminaison local à `localhost:9000/2015-03-31/functions/function/invocations`.

> **Note**
>
> Si vous avez créé l'image Docker pour l'architecture du jeu d'instructions ARM64, veillez à utiliser l'option `--platform linux/arm64` plutôt que `--platform linux/amd64`.

2. À partir d'une nouvelle fenêtre de terminal, publiez un événement au point de terminaison local.

Linux/macOS

Sous Linux et macOS, exécutez la commande `curl` suivante :

```
curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d '{}'
```

Cette commande invoque la fonction avec un événement vide et renvoie une réponse. Si vous utilisez votre propre code de fonction plutôt que l'exemple de code de fonction, vous pouvez invoquer la fonction avec une charge utile JSON. Exemple :

```
curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d
 '{"payload":"hello world!"}'
```

PowerShell

Dans PowerShell, exécutez la `Invoke-WebRequest` commande suivante :

```
Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/
invocations" -Method Post -Body '{}' -ContentType "application/json"
```

Cette commande invoque la fonction avec un événement vide et renvoie une réponse. Si vous utilisez votre propre code de fonction plutôt que l'exemple de code de fonction, vous pouvez invoquer la fonction avec une charge utile JSON. Exemple :

```
Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/
invocations" -Method Post -Body '{"payload":"hello world!"}' -ContentType
 "application/json"
```

3. Obtenez l'ID du conteneur.

```
docker ps
```

4. Utilisez la commande docker kill pour arrêter le conteneur. Dans cette commande, remplacez `3766c4ab331c` par l'ID du conteneur de l'étape précédente.

```
docker kill 3766c4ab331c
```

Déploiement de l'image

Pour charger l'image sur Amazon RIE et créer la fonction Lambda

1. Exécutez la commande get-login-password pour authentifier la CLI Docker auprès de votre registre Amazon ECR.
   - Définissez la `--region` valeur à l' Région AWS endroit où vous souhaitez créer le référentiel Amazon ECR.
   - `111122223333`Remplacez-le par votre Compte AWS identifiant.

```
aws ecr get-login-password --region us-east-1 | docker login --username AWS --
password-stdin 111122223333.dkr.ecr.us-east-1.amazonaws.com
```

2. Créez un référentiel dans Amazon ECR à l'aide de la commande create-repository.

```
aws ecr create-repository --repository-name hello-world --region us-east-1 --image-
scanning-configuration scanOnPush=true --image-tag-mutability MUTABLE
```

> **Note**
>
> Le référentiel Amazon ECR doit être Région AWS identique à la fonction Lambda.

En cas de succès, vous obtenez une réponse comme celle-ci :

```
{
    "repository": {
        "repositoryArn": "arn:aws:ecr:us-east-1:111122223333:repository/hello-
world",
        "registryId": "111122223333",
        "repositoryName": "hello-world",
        "repositoryUri": "111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-
world",
        "createdAt": "2023-03-09T10:39:01+00:00",
        "imageTagMutability": "MUTABLE",
        "imageScanningConfiguration": {
            "scanOnPush": true
        },
        "encryptionConfiguration": {
            "encryptionType": "AES256"
        }
    }
}
```

3. Copiez le `repositoryUri` à partir de la sortie de l'étape précédente.
4. Exécutez la commande docker tag pour étiqueter votre image locale dans votre référentiel Amazon ECR en tant que dernière version. Dans cette commande :

   - `docker-image:test` est le nom et la balise de votre image Docker. Il s'agit du nom et de la balise de l'image que vous avez spécifiés dans la commande `docker build`.
   - Remplacez <ECRrepositoryUri> par l'`repositoryUri` que vous avez copié. Assurez-vous d'inclure `:latest` à la fin de l'URI.

```
docker tag docker-image:test <ECRrepositoryUri>:latest
```

Exemple :

```
docker tag docker-image:test 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

5. Exécutez la commande docker push pour déployer votre image locale dans le référentiel Amazon ECR. Assurez-vous d'inclure `:latest` à la fin de l'URI du référentiel.

```
docker push 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

6. Créez un rôle d'exécution pour la fonction, si vous n'en avez pas déjà un. Vous aurez besoin de l'Amazon Resource Name (ARN) du rôle à l'étape suivante.
7. Créez la fonction Lambda. Pour `ImageUri`, indiquez l'URI du référentiel mentionné précédemment. Assurez-vous d'inclure `:latest` à la fin de l'URI.

```
aws lambda create-function \
  --function-name hello-world \
  --package-type Image \
  --code ImageUri=111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \
  --role arn:aws:iam::111122223333:role/lambda-ex
```

> **Note**
>
> Vous pouvez créer une fonction en utilisant une image d'un autre AWS compte, à condition que l'image se trouve dans la même région que la fonction Lambda. Pour plus d'informations, consultez Autorisations entre comptes Amazon ECR.

8. Invoquer la fonction.

```
aws lambda invoke --function-name hello-world response.json
```

Vous devriez obtenir une réponse comme celle-ci :

```
{
  "ExecutedVersion": "$LATEST",
```

```
  "StatusCode": 200
}
```

9. Pour voir la sortie de la fonction, consultez le fichier `response.json`.

Pour mettre à jour le code de la fonction, vous devez recréer l'image, charger la nouvelle image dans le référentiel Amazon ECR, puis utiliser la commande update-function-code pour déployer l'image dans la fonction Lambda.

Lambda résout l'étiquette d'image en hachage d'image spécifique. Cela signifie que si vous pointez la balise d'image qui a été utilisée pour déployer la fonction vers une nouvelle image dans Amazon ECR, Lambda ne met pas automatiquement à jour la fonction pour utiliser la nouvelle image.

Pour déployer la nouvelle image sur la même fonction Lambda, vous devez utiliser la commande update-function-code, même si la balise d'image dans Amazon ECR reste la même. Dans l'exemple suivant, l'option `--publish` crée une version de la fonction à l'aide de l'image du conteneur mise à jour.

```
aws lambda update-function-code \
  --function-name hello-world \
  --image-uri 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \
  --publish
```

Utilisation de l'objet de contexte Lambda pour récupérer les informations de la fonction TypeScript d'événement

Lorsque Lambda exécute votre fonction d'événement, elle transmet un objet de contexte au gestionnaire. Cet objet fournit des méthodes et des propriétés fournissant des informations sur l'invocation, la fonction et l'environnement d'exécution.

Pour activer la vérification de type pour l'objet de contexte, vous devez ajouter le package @ types/ aws -lambda en tant que dépendance de développement et importer le `Context` type. Pour plus d'informations, consultez Définitions de type pour Lambda.

Méthodes de contexte

- `getRemainingTimeInMillis()` – Renvoie le nombre de millisecondes restant avant l'expiration de l'exécution.

Propriétés du contexte

- `functionName` – Nom de la fonction Lambda.
- `functionVersion` – Version de la fonction.
- `invokedFunctionArn` – Amazon Resource Name (ARN) utilisé pour appeler la fonction. Indique si l'appelant a spécifié un numéro de version ou un alias.
- `memoryLimitInMB` – Quantité de mémoire allouée à la fonction.
- `awsRequestId` – Identifiant de la demande d'invocation.
- `logGroupName` – Groupe de journaux pour la fonction.
- `logStreamName` – Flux de journal de l'instance de fonction.
- `identity` – (applications mobiles) Informations sur l'identité Amazon Cognito qui a autorisé la demande.
  - `cognitoIdentityId` – Identité Amazon Cognito authentifiée.
  - `cognitoIdentityPoolId` – Groupe d'identités Amazon Cognito ayant autorisé l'invocation.
- `clientContext` – (applications mobiles) Contexte client fourni à Lambda par l'application client.
  - `client.installation_id`
  - `client.app_title`
  - `client.app_version_name`
  - `client.app_version_code`

  - `client.app_package_name`
  - `env.platform_version`
  - `env.platform`
  - `env.make`
  - `env.model`
  - `env.locale`
  - `Custom` – Personnalisez les valeurs qui sont définies par l'application client.
- `callbackWaitsForEmptyEventLoop`— Par défaut (`true`), lors de l'utilisation d'un gestionnaire de fonctions basé sur le rappel, Lambda attend que la boucle d'événements soit vide après l'exécution du rappel avant de terminer l'appel de la fonction. Définissez cette valeur `false` sur pour envoyer la réponse et mettre fin à l'appel immédiatement après l'exécution du rappel au lieu d'attendre que la boucle d'événements soit vide. Les événements exceptionnels continuent de se dérouler lors de la prochaine invocation. Notez que Lambda prend en charge les gestionnaires de fonctions basés sur le rappel uniquement pour les environnements d'exécution Node.js 22 et antérieurs.

Example Fichier index.ts

Dans l'exemple suivant, la fonction enregistre des informations de contexte et renvoie l'emplacement des journaux.

> **Note**
>
> Avant d'utiliser ce code dans une fonction Lambda, vous devez ajouter le package @ types/ aws -lambda en tant que dépendance de développement. Ce package contient les définitions de type pour Lambda. Pour plus d'informations, consultez Définitions de type pour Lambda.

```
import { Context } from 'aws-lambda';
export const lambdaHandler = async (event: string, context: Context): Promise<string>
 => {
  console.log('Remaining time: ', context.getRemainingTimeInMillis());
  console.log('Function name: ', context.functionName);
  return context.logStreamName;
};
```

Enregistrez et surveillez les fonctions des TypeScript événements Lambda

AWS Lambda surveille automatiquement les fonctions Lambda et envoie des entrées de journal à Amazon. CloudWatch Votre fonction Lambda est fournie avec un groupe de CloudWatch journaux Logs et un flux de journaux pour chaque instance de votre fonction. L'environnement d'exécution Lambda envoie des détails sur chaque invocation et d'autres sorties provenant du code de votre fonction au flux de journaux. Pour plus d'informations sur CloudWatch les journaux, consultezEnvoi des journaux des fonctions d'événements Lambda aux journaux CloudWatch.

Pour générer les journaux à partir de votre code de fonction, vous pouvez utiliser des méthodes sur l'objet console. Pour une journalisation plus détaillée, vous pouvez utiliser n'importe quelle bibliothèque de journalisation qui écrit dans `stdout` ou `stderr`.

Sections

- Utilisation d'outils et de bibliothèques de journalisation
- Utilisation de Powertools pour AWS Lambda (TypeScript) et AWS SAM pour une journalisation structurée
- Utilisation de Powertools pour AWS Lambda (TypeScript) et le AWS CDK pour une journalisation structurée
- Affichage des journaux dans la console Lambda
- Afficher les journaux dans la CloudWatch console

Utilisation d'outils et de bibliothèques de journalisation

Powertools for AWS Lambda (TypeScript) est une boîte à outils destinée aux développeurs qui permet de mettre en œuvre les meilleures pratiques sans serveur et d'accroître la rapidité des développeurs. L'utilitaire Logger fournit un enregistreur optimisé pour Lambda qui inclut des informations supplémentaires sur le contexte de fonction pour toutes vos fonctions avec une sortie structurée en JSON. Utilisez cet utilitaire pour effectuer les opérations suivantes :

- Capturer les champs clés du contexte Lambda, démarrer à froid et structurer la sortie de la journalisation sous forme de JSON
- Journaliser les événements d'invocation Lambda lorsque cela est demandé (désactivé par défaut)
- Imprimer tous les journaux uniquement pour un pourcentage d'invocations via l'échantillonnage des journaux (désactivé par défaut)
- Ajouter des clés supplémentaires au journal structuré à tout moment

- Utiliser un formateur de journaux personnalisé (Apportez votre propre formateur) pour produire des journaux dans une structure compatible avec le RFC de journalisation de votre organisation

Utilisation de Powertools pour AWS Lambda (TypeScript) et AWS SAM pour une journalisation structurée

Suivez les étapes ci-dessous pour télécharger, créer et déployer un exemple d' TypeScript application Hello World avec des modules Powertools for AWS Lambda (TypeScript) intégrés à l'aide du AWS SAM. Cette application met en œuvre un backend API de base et utilise Powertools pour émettre des journaux, des métriques et des traces. Elle se compose d'un point de terminaison Amazon API Gateway et d'une fonction Lambda. Lorsque vous envoyez une requête GET au point de terminaison API Gateway, la fonction Lambda appelle, envoie des journaux et des métriques au format métrique intégré à CloudWatch, et envoie des traces à. AWS X-Ray La fonction renvoie un message `hello world`.

Conditions préalables

Pour exécuter la procédure indiquée dans cette section, vous devez satisfaire aux exigences suivantes :

- Node.js 20 ou version ultérieure
- AWS CLI version 2
- AWS SAM CLI version 1.75 ou ultérieure. Si vous disposez d'une ancienne version de la AWS SAM CLI, reportez-vous à la section Mise à niveau de la AWS SAM CLI.

Déployer un échantillon AWS SAM vigie

1. Initialisez l'application à l'aide du TypeScript modèle Hello World.

```
sam init --app-template hello-world-powertools-typescript --name sam-app --package-type Zip --runtime nodejs24.x
```

2. Créez l'application.

```
cd sam-app && sam build
```

3. Déployez l'application.

```
sam deploy --guided
```

4. Suivez les invites à l'écran. Appuyez sur `Enter` pour accepter les options par défaut fournies dans l'expérience interactive.

> **Note**
>
> Car l'autorisation n'a HelloWorldFunction peut-être pas été définie, est-ce que ça va ? , assurez-vous de participery.

5. Obtenez l'URL de l'application déployée :

```
aws cloudformation describe-stacks --stack-name sam-app --query
 'Stacks[0].Outputs[?OutputKey==`HelloWorldApi`].OutputValue' --output text
```

6. Invoquez le point de terminaison de l'API :

```
curl <URL_FROM_PREVIOUS_STEP>
```

En cas de succès, vous obtiendrez cette réponse :

```
{"message":"hello world"}
```

7. Pour obtenir les journaux de la fonction, exécutez sam logs. Pour en savoir plus, consultez Utilisation des journaux dans le Guide du développeur AWS Serverless Application Model .

```
sam logs --stack-name sam-app
```

La sortie du journal se présente comme suit :

```
2025/01/31/[$LATEST]4d53e8d279824834a1ccd35511a4949c 2025-08-31T09:33:10.552000
 START RequestId: 70693159-7e94-4102-a2af-98a6343fb8fb Version: $LATEST
2025/01/31/[$LATEST]4d53e8d279824834a1ccd35511a4949c 2025-08-31T09:33:10.594000
 2025-08-31T09:33:10.557Z 70693159-7e94-4102-a2af-98a6343fb8fb
 INFO {"_aws":{"Timestamp":1661938390556,"CloudWatchMetrics":
[{"Namespace":"sam-app","Dimensions":[["service"]],"Metrics":
[{"Name":"ColdStart","Unit":"Count"}]}]},"service":"helloWorld","ColdStart":1}
2025/01/31/[$LATEST]4d53e8d279824834a1ccd35511a4949c 2025-08-31T09:33:10.595000
 2025-08-31T09:33:10.595Z 70693159-7e94-4102-a2af-98a6343fb8fb INFO
```

```
 {"level":"INFO","message":"This is an INFO log - sending HTTP 200 - hello world
 response","service":"helloWorld","timestamp":"2025-08-31T09:33:10.594Z"}
2025/01/31/[$LATEST]4d53e8d279824834a1ccd35511a4949c 2025-08-31T09:33:10.655000
 2025-08-31T09:33:10.655Z 70693159-7e94-4102-a2af-98a6343fb8fb INFO
 {"_aws":{"Timestamp":1661938390655,"CloudWatchMetrics":[{"Namespace":"sam-
app","Dimensions":[["service"]],"Metrics":[]}]},"service":"helloWorld"}
2025/01/31/[$LATEST]4d53e8d279824834a1ccd35511a4949c 2025-08-31T09:33:10.754000 END
 RequestId: 70693159-7e94-4102-a2af-98a6343fb8fb
2025/01/31/[$LATEST]4d53e8d279824834a1ccd35511a4949c 2025-08-31T09:33:10.754000
 REPORT RequestId: 70693159-7e94-4102-a2af-98a6343fb8fb Duration: 201.55 ms Billed
 Duration: 202 ms Memory Size: 128 MB Max Memory Used: 66 MB Init Duration: 252.42
 ms
XRAY TraceId: 1-630f2ad5-1de22b6d29a658a466e7ecf5 SegmentId: 567c116658fbf11a
 Sampled: true
```

8. Il s’agit d’un point de terminaison d’API public accessible par Internet. Nous vous recommandons de supprimer le point de terminaison après un test.

```
sam delete
```

Gestion de la conservation des journaux

Les groupes de journaux ne sont pas supprimés automatiquement quand vous supprimez une fonction. Pour éviter de stocker les journaux indéfiniment, supprimez le groupe de journaux ou configurez une période de conservation après laquelle les journaux CloudWatch sont automatiquement supprimés. Pour configurer la conservation des journaux, ajoutez ce qui suit à votre AWS SAM modèle :

```
Resources:
  HelloWorldFunction:
    Type: AWS::Serverless::Function
    Properties:
    # Omitting other properties

  LogGroup:
    Type: AWS::Logs::LogGroup
    Properties:
      LogGroupName: !Sub "/aws/lambda/${HelloWorldFunction}"
      RetentionInDays: 7
```

Utilisation de Powertools pour AWS Lambda (TypeScript) et le AWS CDK pour une journalisation structurée

Suivez les étapes ci-dessous pour télécharger, créer et déployer un exemple d' TypeScript application Hello World avec des modules Powertools for AWS Lambda (TypeScript) intégrés à l'aide du AWS CDK. Cette application met en œuvre un backend API de base et utilise Powertools pour émettre des journaux, des métriques et des traces. Elle se compose d'un point de terminaison Amazon API Gateway et d'une fonction Lambda. Lorsque vous envoyez une requête GET au point de terminaison API Gateway, la fonction Lambda appelle, envoie des journaux et des métriques au format métrique intégré à CloudWatch, et envoie des traces à. AWS X-Ray La fonction renvoie un message `hello world`.

Conditions préalables

Pour exécuter la procédure indiquée dans cette section, vous devez satisfaire aux exigences suivantes :

- Node.js 20 ou version ultérieure
- AWS CLI version 2
- AWS CDK version 2
- AWS SAM CLI version 1.75 ou ultérieure. Si vous disposez d'une ancienne version de la AWS SAM CLI, reportez-vous à la section Mise à niveau de la AWS SAM CLI.

Déployer un échantillon AWS CDK vigie

1. Créez un répertoire de projets pour votre nouvelle application.

```
mkdir hello-world
cd hello-world
```

2. Initialisez l'application.

```
cdk init app --language typescript
```

3. Ajoutez le package @ types/aws -lambda en tant que dépendance de développement.

```
npm install -D @types/aws-lambda
```

4. Installez l'utilitaire Powertools Logger (français non garanti).

```
npm install @aws-lambda-powertools/logger
```

5. Ouvrez le répertoire lib. Vous devriez voir un fichier nommé hello-world-stack.ts. Créez deux nouveaux fichiers dans ce répertoire : hello-world.function.ts et hello-world.ts.
6. Ouvrez hello-world.function.ts et ajoutez le code suivant au fichier. Il s'agit du code de la fonction Lambda.

```
import { APIGatewayEvent, APIGatewayProxyResult, Context } from 'aws-lambda';
import { Logger } from '@aws-lambda-powertools/logger';
const logger = new Logger();

export const handler = async (event: APIGatewayEvent, context: Context):
 Promise<APIGatewayProxyResult> => {
  logger.info('This is an INFO log - sending HTTP 200 - hello world response');
  return {
    statusCode: 200,
    body: JSON.stringify({
      message: 'hello world',
    }),
  };
};
```

7. Ouvrez hello-world.ts et ajoutez le code suivant au fichier. Il contient la NodejsFunction construction qui crée la fonction Lambda, configure les variables d'environnement pour Powertools et définit la durée de conservation des journaux à une semaine. Il inclut également la LambdaRestApi construction qui crée l'API REST.

```
import { Construct } from 'constructs';
import { NodejsFunction } from 'aws-cdk-lib/aws-lambda-nodejs';
import { LambdaRestApi } from 'aws-cdk-lib/aws-apigateway';
import { RetentionDays } from 'aws-cdk-lib/aws-logs';
import { CfnOutput } from 'aws-cdk-lib';

export class HelloWorld extends Construct {
  constructor(scope: Construct, id: string) {
    super(scope, id);
    const helloFunction = new NodejsFunction(this, 'function', {
      environment: {
        Powertools_SERVICE_NAME: 'helloWorld',
        LOG_LEVEL: 'INFO',
      },
```

```
      logRetention: RetentionDays.ONE_WEEK,
    });
    const api = new LambdaRestApi(this, 'apigw', {
      handler: helloFunction,
    });
    new CfnOutput(this, 'apiUrl', {
      exportName: 'apiUrl',
      value: api.url,
    });
  }
}
```

8. Ouvrez hello-world stack.ts. C'est le code qui définit votre pile de AWS CDK. Remplacez le code par ce qui suit :

```
import { Stack, StackProps } from 'aws-cdk-lib';
import { Construct } from 'constructs';
import { HelloWorld } from './hello-world';

export class HelloWorldStack extends Stack {
  constructor(scope: Construct, id: string, props?: StackProps) {
    super(scope, id, props);
    new HelloWorld(this, 'hello-world');
  }
}
```

9. Revenez au répertoire du projet.

```
cd hello-world
```

10. Déployez votre application.

```
cdk deploy
```

11. Obtenez l'URL de l'application déployée :

```
aws cloudformation describe-stacks --stack-name HelloWorldStack --query
 'Stacks[0].Outputs[?ExportName==`apiUrl`].OutputValue' --output text
```

12. Invoquez le point de terminaison de l'API :

```
curl <URL_FROM_PREVIOUS_STEP>
```

En cas de succès, vous obtiendrez cette réponse :

```
{"message":"hello world"}
```

13. Pour obtenir les journaux de la fonction, exécutez sam logs. Pour en savoir plus, consultez Utilisation des journaux dans le Guide du développeur AWS Serverless Application Model .

```
sam logs --stack-name HelloWorldStack
```

La sortie du journal se présente comme suit :

```
2025/01/31/[$LATEST]2ca67f180dcd4d3e88b5d68576740c8e 2025-08-31T14:48:37.047000
 START RequestId: 19ad1007-ff67-40ce-9afe-0af0a9eb512c Version: $LATEST
2025/01/31/[$LATEST]2ca67f180dcd4d3e88b5d68576740c8e 2025-08-31T14:48:37.050000 {
"level": "INFO",
"message": "This is an INFO log - sending HTTP 200 - hello world response",
"service": "helloWorld",
"timestamp": "2025-08-31T14:48:37.048Z",
"xray_trace_id": "1-630f74c4-2b080cf77680a04f2362bcf2"
}
2025/01/31/[$LATEST]2ca67f180dcd4d3e88b5d68576740c8e 2025-08-31T14:48:37.082000 END
 RequestId: 19ad1007-ff67-40ce-9afe-0af0a9eb512c
2025/01/31/[$LATEST]2ca67f180dcd4d3e88b5d68576740c8e 2025-08-31T14:48:37.082000
 REPORT RequestId: 19ad1007-ff67-40ce-9afe-0af0a9eb512c Duration: 34.60 ms Billed
 Duration: 35 ms Memory Size: 128 MB Max Memory Used: 57 MB Init Duration: 173.48
 ms
```

14. Il s’agit d’un point de terminaison d’API public accessible par Internet. Nous vous recommandons de supprimer le point de terminaison après un test.

```
cdk destroy
```

Affichage des journaux dans la console Lambda

Vous pouvez utiliser la console Lambda pour consulter les résultats du journal après avoir invoqué une fonction d'événement Lambda.

Si votre code peut être testé à partir de l'éditeur de code intégré, vous trouverez des journaux dans les résultats d'exécution. Lorsque vous utilisez la fonctionnalité de test de la console pour appeler une fonction, vous trouverez la sortie du journal dans la section Détails.

Afficher les journaux dans la CloudWatch console

Vous pouvez utiliser la CloudWatch console Amazon pour consulter les journaux de toutes les invocations de la fonction d'événement Lambda.

Pour afficher les journaux sur la CloudWatch console

1. Ouvrez la page Groupes de journaux sur la CloudWatch console.
2. Choisissez le groupe de journaux pour votre fonction (/aws/lambda/***your-function-name***).
3. Choisissez un flux de journaux.

Chaque flux de journal correspond à une instance de votre fonction. Un flux de journal apparaît lorsque vous mettez à jour votre fonction Lambda et lorsque des instances supplémentaires sont créées pour gérer les appels simultanés. Pour trouver les journaux d'un appel spécifique, nous vous recommandons d'instrumenter votre fonction avec. AWS X-Ray X-Ray enregistre les détails de la demande et du flux de log dans le traçage.

TypeScript Code de suivi dans AWS Lambda

Lambda s'intègre pour vous aider AWS X-Ray à suivre, à déboguer et à optimiser les applications Lambda. Vous pouvez l'utiliser X-Ray pour suivre une demande lorsqu'elle parcourt les ressources de votre application, ce qui peut inclure des fonctions Lambda et AWS d'autres services.

Pour envoyer des données de suivi à X-Ray, vous pouvez utiliser l'une des trois bibliothèques du SDK :

- AWS Distro for OpenTelemetry (ADOT) — Une distribution sécurisée, prête pour la production et prise AWS en charge du SDK (OTel). OpenTelemetry
- AWS X-Ray SDK pour Node.js : SDK permettant de générer et d'envoyer des données de suivi à. X-Ray
- Powertools for AWS Lambda (TypeScript) — Une boîte à outils pour les développeurs permettant de mettre en œuvre les meilleures pratiques sans serveur et d'accroître la rapidité des développeurs.

Chacun des SDK propose des moyens d'envoyer vos données de télémétrie au service. X-Ray Vous pouvez ensuite les utiliser X-Ray pour afficher, filtrer et obtenir des informations sur les indicateurs de performance de votre application afin d'identifier les problèmes et les opportunités d'optimisation.

> **Important**
>
> Les X-Ray et Powertools for AWS Lambda SDK font partie d'une solution d'instrumentation étroitement intégrée proposée par. AWS Les couches ADOT Lambda font partie d’une norme industrielle pour l’instrumentation de traçage qui collecte plus de données en général, mais qui peut ne pas convenir à tous les cas d’utilisation. Vous pouvez implémenter le suivi de bout en bout à l' X-Ray aide de l'une ou l'autre solution. Pour en savoir plus sur le choix entre les deux, voir Choisir entre la AWS distribution pour Open Telemetry et les SDK. X-Ray

Sections

- Utilisation de Powertools pour AWS Lambda (TypeScript) et AWS SAM pour le traçage
- Utilisation de Powertools pour AWS Lambda (TypeScript) et le AWS CDK pour le traçage
- Interprétation et X-Ray traçage

Utilisation de Powertools pour AWS Lambda (TypeScript) et AWS SAM pour le traçage

Suivez les étapes ci-dessous pour télécharger, créer et déployer un exemple d' TypeScript application Hello World avec des modules Powertools for AWS Lambda (TypeScript) intégrés à l'aide du AWS SAM. Cette application met en œuvre un backend API de base et utilise Powertools pour émettre des journaux, des métriques et des traces. Elle se compose d'un point de terminaison Amazon API Gateway et d'une fonction Lambda. Lorsque vous envoyez une requête GET au point de terminaison API Gateway, la fonction Lambda appelle, envoie des journaux et des métriques au format métrique intégré à CloudWatch, et envoie des traces à. AWS X-Ray La fonction renvoie un message `hello world`.

Conditions préalables

Pour exécuter la procédure indiquée dans cette section, vous devez satisfaire aux exigences suivantes :

- Node.js
- AWS CLI version 2
- AWS SAM CLI version 1.75 ou ultérieure. Si vous disposez d'une ancienne version de la AWS SAM CLI, reportez-vous à la section Mise à niveau de la AWS SAM CLI.

Déployer un échantillon AWS SAM vigie

1. Initialisez l'application à l'aide du TypeScript modèle Hello World.

```
sam init --app-template hello-world-powertools-typescript --name sam-app --package-type Zip --runtime nodejs24.x --no-tracing
```

2. Créez l'application.

```
cd sam-app && sam build
```

3. Déployez l'application.

```
sam deploy --guided
```

4. Suivez les invites à l'écran. Appuyez sur `Enter` pour accepter les options par défaut fournies dans l'expérience interactive.

> **Note**
>
> Car l'autorisation n'a HelloWorldFunction peut-être pas été définie, est-ce que ça va ? , assurez-vous de participery.

5. Obtenez l'URL de l'application déployée :

```
aws cloudformation describe-stacks --stack-name sam-app --query
 'Stacks[0].Outputs[?OutputKey==`HelloWorldApi`].OutputValue' --output text
```

6. Invoquez le point de terminaison de l'API :

```
curl <URL_FROM_PREVIOUS_STEP>
```

   En cas de succès, vous obtiendrez cette réponse :

```
{"message":"hello world"}
```

7. Pour obtenir les traces de la fonction, exécutez sam traces.

```
sam traces
```

   La sortie de la trace ressemble à ceci :

```
XRay Event [revision 1] at (2023-01-31T11:29:40.527000) with id
 (1-11a2222-111a222222cb33de3b95daf9) and duration (0.483s)
  - 0.425s - sam-app/Prod [HTTP: 200]
    - 0.422s - Lambda [HTTP: 200]
  - 0.406s - sam-app-HelloWorldFunction-Xyzv11a1bcde [HTTP: 200]
  - 0.172s - sam-app-HelloWorldFunction-Xyzv11a1bcde
    - 0.179s - Initialization
    - 0.112s - Invocation
      - 0.052s - ## app.lambdaHandler
        - 0.001s - ### MySubSegment
    - 0.059s - Overhead
```

8. Il s'agit d'un point de terminaison d'API public accessible par Internet. Nous vous recommandons de supprimer le point de terminaison après un test.

```
sam delete
```

X-Ray n'assure pas le suivi de toutes les demandes jusqu'à votre application. X-Ray applique un algorithme d'échantillonnage pour garantir l'efficacité du suivi, tout en fournissant un échantillon représentatif de toutes les demandes. Le taux d'échantillonnage est 1 demande par seconde et 5 % de demandes supplémentaires. Vous ne pouvez pas configurer le taux X-Ray d'échantillonnage pour vos fonctions.

Utilisation de Powertools pour AWS Lambda (TypeScript) et le AWS CDK pour le traçage

Suivez les étapes ci-dessous pour télécharger, créer et déployer un exemple d' TypeScript application Hello World avec des modules Powertools for AWS Lambda (TypeScript) intégrés à l'aide du AWS CDK. Cette application met en œuvre un backend API de base et utilise Powertools pour émettre des journaux, des métriques et des traces. Elle se compose d'un point de terminaison Amazon API Gateway et d'une fonction Lambda. Lorsque vous envoyez une requête GET au point de terminaison API Gateway, la fonction Lambda appelle, envoie des journaux et des métriques au format métrique intégré à CloudWatch, et envoie des traces à. AWS X-Ray La fonction renvoie un message `hello world`.

Conditions préalables

Pour exécuter la procédure indiquée dans cette section, vous devez satisfaire aux exigences suivantes :

- Node.js
- AWS CLI version 2
- AWS CDK version 2
- AWS SAM CLI version 1.75 ou ultérieure. Si vous disposez d'une ancienne version de la AWS SAM CLI, reportez-vous à la section Mise à niveau de la AWS SAM CLI.

Déployer un échantillon Cloud Development Kit AWS (AWS CDK) vigie

1. Créez un répertoire de projets pour votre nouvelle application.

```
mkdir hello-world
cd hello-world
```

2. Initialisez l'application.

```
cdk init app --language typescript
```

3. Ajoutez le package @ types/aws -lambda en tant que dépendance de développement.

```
npm install -D @types/aws-lambda
```

4. Installez l'utilitaire Powertools Tracer.

```
npm install @aws-lambda-powertools/tracer
```

5. Ouvrez le répertoire lib. Vous devriez voir un fichier nommé hello-world-stack.ts. Créez deux nouveaux fichiers dans ce répertoire : hello-world.function.ts et hello-world.ts.

6. Ouvrez hello-world.function.ts et ajoutez le code suivant au fichier. Il s'agit du code de la fonction Lambda.

```
import { APIGatewayEvent, APIGatewayProxyResult, Context } from 'aws-lambda';
import { Tracer } from '@aws-lambda-powertools/tracer';
const tracer = new Tracer();

export const handler = async (event: APIGatewayEvent, context: Context):
 Promise<APIGatewayProxyResult> => {
  // Get facade segment created by Lambda
  const segment = tracer.getSegment();

  // Create subsegment for the function and set it as active
  const handlerSegment = segment.addNewSubsegment(`## ${process.env._HANDLER}`);
  tracer.setSegment(handlerSegment);

  // Annotate the subsegment with the cold start and serviceName
  tracer.annotateColdStart();
  tracer.addServiceNameAnnotation();

  // Add annotation for the awsRequestId
  tracer.putAnnotation('awsRequestId', context.awsRequestId);
  // Create another subsegment and set it as active
  const subsegment = handlerSegment.addNewSubsegment('### MySubSegment');
  tracer.setSegment(subsegment);
  let response: APIGatewayProxyResult = {
    statusCode: 200,
    body: JSON.stringify({
```

```
      message: 'hello world',
    }),
  };
  // Close subsegments (the Lambda one is closed automatically)
  subsegment.close(); // (### MySubSegment)
  handlerSegment.close(); // (## index.handler)

  // Set the facade segment as active again (the one created by Lambda)
  tracer.setSegment(segment);
  return response;
};
```

7. Ouvrez hello-world.ts et ajoutez le code suivant au fichier. Il contient la NodejsFunction construction qui crée la fonction Lambda, configure les variables d'environnement pour Powertools et définit la durée de conservation des journaux à une semaine. Il inclut également la LambdaRestApi construction qui crée l'API REST.

```
import { Construct } from 'constructs';
import { NodejsFunction } from 'aws-cdk-lib/aws-lambda-nodejs';
import { LambdaRestApi } from 'aws-cdk-lib/aws-apigateway';
import { CfnOutput } from 'aws-cdk-lib';
import { Tracing } from 'aws-cdk-lib/aws-lambda';

export class HelloWorld extends Construct {
  constructor(scope: Construct, id: string) {
    super(scope, id);
    const helloFunction = new NodejsFunction(this, 'function', {
      environment: {
        POWERTOOLS_SERVICE_NAME: 'helloWorld',
      },
      tracing: Tracing.ACTIVE,
    });
    const api = new LambdaRestApi(this, 'apigw', {
      handler: helloFunction,
    });
    new CfnOutput(this, 'apiUrl', {
      exportName: 'apiUrl',
      value: api.url,
    });
  }
}
```

8. Ouvrez hello-world stack.ts. C'est le code qui définit votre pile de AWS CDK. Remplacez le code par ce qui suit :

```
import { Stack, StackProps } from 'aws-cdk-lib';
import { Construct } from 'constructs';
import { HelloWorld } from './hello-world';

export class HelloWorldStack extends Stack {
  constructor(scope: Construct, id: string, props?: StackProps) {
    super(scope, id, props);
    new HelloWorld(this, 'hello-world');
  }
}
```

9. Déployez votre application.

```
cd ..
cdk deploy
```

10. Obtenez l'URL de l'application déployée :

```
aws cloudformation describe-stacks --stack-name HelloWorldStack --query
 'Stacks[0].Outputs[?ExportName==`apiUrl`].OutputValue' --output text
```

11. Invoquez le point de terminaison de l'API :

```
curl <URL_FROM_PREVIOUS_STEP>
```

    En cas de succès, vous obtiendrez cette réponse :

```
{"message":"hello world"}
```

12. Pour obtenir les traces de la fonction, exécutez sam traces.

```
sam traces
```

    La sortie de la trace ressemble à ceci :

```
XRay Event [revision 1] at (2023-01-31T11:50:06.997000) with id
 (1-11a2222-111a222222cb33de3b95daf9) and duration (0.449s)
  - 0.350s - HelloWorldStack-helloworldfunction111A2BCD-Xyzv11a1bcde [HTTP: 200]
```

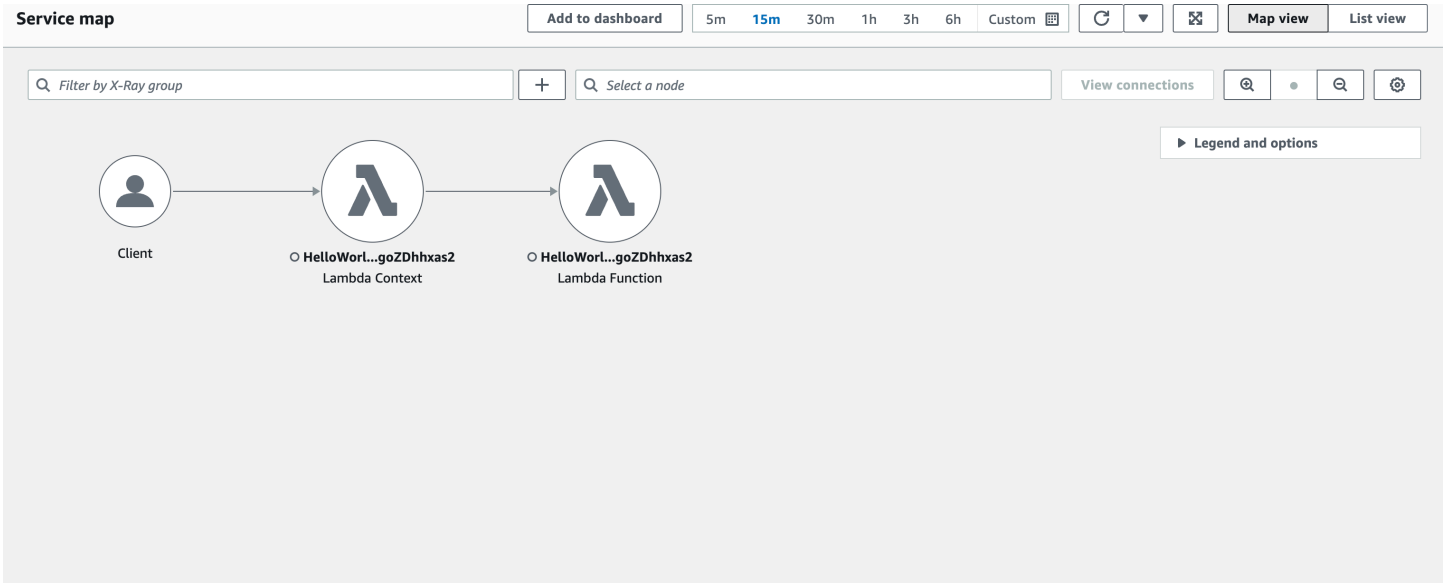
```
  - 0.157s - HelloWorldStack-helloworldfunction111A2BCD-Xyzv11a1bcde
    - 0.169s - Initialization
    - 0.058s - Invocation
      - 0.055s - ## index.handler
        - 0.000s - ### MySubSegment
    - 0.099s - Overhead
```

13. Il s'agit d'un point de terminaison d'API public accessible par Internet. Nous vous recommandons de supprimer le point de terminaison après un test.

```
cdk destroy
```

Interprétation et X-Ray traçage

Une fois que vous avez configuré le suivi actif, vous pouvez observer des demandes spécifiques via votre application. La carte de X-Ray trace fournit des informations sur votre application et tous ses composants. L'exemple suivant montre une trace à partir de l'exemple d'application :



Création de fonctions d'événement Lambda avec Python

Vous pouvez exécuter du code Python dans AWS Lambda Event Functions. Lambda fournit des runtimes pour Python qui exécutent votre code afin de traiter des événements. Votre code s'exécute dans un environnement qui inclut le SDK pour Python (Boto3), avec les informations d'identification d'un rôle (IAM) que vous Gestion des identités et des accès AWS gérez. Pour en savoir plus sur les versions du kit SDK incluses dans les environnements d'exécution Python, consultez the section called "Runtime-included Versions du SDK".

Lambda prend en charge les runtimes Python suivants.

Nom	Identifiant	Système d'exploitation	Date d'obsolescence	Créer la fonction de blocage	Mettre à jour la fonction de blocage
Python 3.15	`python3.15`	Amazon Linux 2	Non planifié	Non planifié	Non planifié
Python 3.14	`python3.14`	Amazon Linux 2	30 juin 2029	31 juillet 2029	31 août 2029
Python 3.13	`python3.13`	Amazon Linux 2	30 juin 2029	31 juillet 2029	31 août 2029
Python 3.12	`python3.12`	Amazon Linux 2	31 octobre 2028	30 novembre 2028	10 janvier 2029
Python 3.11	`python3.11`	Amazon Linux 2	30 juin 2027	29 juillet 2027	31 août 2027
Python 3.10	`python3.10`	Amazon Linux 2	31 octobre 2026	29 juillet 2027	31 août 2027

Pour créer une fonction d'événement Python

1. Ouvrez la console Lambda.
2. Choisissez Create Event Function.
3. Configurez les paramètres suivants :
   - Nom de la fonction : saisissez le nom de la fonction.
   - Runtime : choisissez Python 3.14.
4. Choisissez Create Event Function.

La console crée une fonction d'événement Lambda avec un seul fichier source nommé. `lambda_function` Vous pouvez modifier ce fichier et ajouter d'autres fichiers dans l'éditeur de code intégré. Dans la section DÉPLOYER, choisissez Déployer pour mettre à jour le code de votre

fonction. Ensuite, pour exécuter votre code, choisissez Créer un événement de test dans la section ÉVÉNEMENTS DE TEST.

Votre fonction Lambda est fournie avec un groupe de CloudWatch journaux Logs. La fonction runtime envoie les détails de chaque appel à CloudWatch Logs. Il relaie tous les journaux que votre fonction génère pendant l'invocation. Si votre fonction renvoie une erreur, Lambda met en forme l'erreur et la renvoie à l'appelant.

Pour obtenir des conseils sur le test de vos fonctions Python, consultezthe section called "Tests".

Rubriques

- Runtime-included Versions du SDK
- Fonctionnalités Python désactivées
- Format de la réponse
- Arrêt progressif pour les extensions
- Définir le gestionnaire de fonctions d'événement Lambda en Python
- Utilisation d'archives de fichiers .zip pour les fonctions événementielles Lambda en Python
- Déployer des fonctions d'événement Lambda en Python avec des images de conteneur
- Utilisation de couches pour les fonctions d'événement Lambda en Python
- Utilisation de l'objet de contexte Lambda pour récupérer les informations de la fonction d'événement Python
- Enregistrez et surveillez les fonctions d'événements Lambda en Python
- AWS Lambda Tests de fonctions événementielles en Python
- Instrumentation du code Python dans AWS Lambda

Runtime-included Versions du SDK

La version du AWS SDK incluse dans le runtime Python dépend de la version d'exécution et de votre Région AWS. Pour trouver la version du SDK incluse dans le moteur d'exécution que vous utilisez, créez une fonction avec le code suivant.

```
import boto3
import botocore

def lambda_handler(event, context):
```

```
print(f'boto3 version: {boto3.__version__}')
print(f'botocore version: {botocore.__version__}')
```

Fonctionnalités Python désactivées

Le tableau suivant répertorie les fonctionnalités Python désactivées dans les environnements d'exécution gérés par Lambda et les images de base de conteneurs pour Python. Ces fonctionnalités doivent être activées lors de la compilation de l'exécutable Python et ne peuvent pas être activées à l'aide d'un indicateur d'exécution. Pour utiliser ces fonctionnalités dans Lambda, vous pouvez déployer votre propre version d'exécution Python avec ces fonctionnalités activées, à l'aide d'une image de conteneur ou d'un environnement d'exécution personnalisé.

Fonctionnalité Python	Versions de Python concernées	Statut
Just-in-Time compilateur (JIT)	Python 3.13 et versions ultérieures	Le compilateur JIT est expérimental et n'est pas recommandé pour les charges de travail de production. Il est donc désactivé dans les environnements d'exécution Lambda Python.
Free-threading	Python 3.13 et versions ultérieures	Le threading gratuit (option permettant de désactiver le verrouillage global de l'interpr éteur) est désactivé dans les versions Lambda Python en raison de l'impact sur les performan ces du code à thread unique.

Format de la réponse

Dans les environnements d'exécution Python 3.12 et versions ultérieures, les fonctions renvoient des caractères Unicode dans le cadre de leur réponse JSON. Les environnements d'exécution Python antérieurs renvoyaient des séquences échappées pour les caractères Unicode dans les réponses. Par exemple, dans Python 3.11, si vous renvoyez une chaîne Unicode telle que « こんにちは », elle échappe le caractères Unicode et renvoie « \u3053\u3093\u306b\u3061\u306f ». L'environnement d'exécution Python 3.12 renvoie le « こんにちは » d'origine.

L'utilisation de réponses Unicode réduit la taille des réponses Lambda, ce qui facilite l'adaptation de réponses plus importantes à la taille de charge utile maximale de 6 Mo pour les fonctions synchrones.

Dans l'exemple précédent, la version échappée est de 32 octets, contre 17 octets pour la chaîne Unicode.

Lors de la mise à niveau vers Python 3.12 ou à une version ultérieure de l'environnement d'exécution Python, vous devrez peut-être ajuster votre code pour tenir compte du nouveau format de réponse. Si l'appelant s'attend à une chaîne Unicode échappée, vous devez soit ajouter du code à la fonction de renvoi pour échapper l'Unicode manuellement, soit ajuster l'appelant pour qu'il gère le retour Unicode.

Arrêt progressif pour les extensions

Les environnements d'exécution Python 3.12 et versions ultérieures offrent des fonctionnalités d'arrêt progressif améliorées pour les fonctions dotées d'extensions externes. Quand Lambda arrête l'exécution, il envoie un signal `SIGTERM` à l'exécution, puis un événement `SHUTDOWN` à chaque extension externe enregistrée. Vous pouvez intercepter le `SIGTERM` signal dans votre fonction et nettoyer les ressources telles que les connexions de base de données créées par la fonction.

Pour en savoir plus sur le cycle de vie de l'environnement d'exécution, veuillez consulter Comprendre le cycle de vie de l'environnement d'exécution Lambda. Pour des exemples d'utilisation de l'arrêt progressif avec des extensions, consultez le GitHub référentiel AWS Samples.

Définir le gestionnaire de fonctions d'événement Lambda en Python

Le gestionnaire de fonctions d'événement Lambda est la méthode de votre code de fonction qui traite les événements. Lorsque votre fonction est invoquée, Lambda exécute la méthode du gestionnaire. Votre fonction s'exécute jusqu'à ce que le gestionnaire renvoie une réponse, se ferme ou expire.

Cette page explique comment utiliser les gestionnaires de fonctions Lambda dans Python, notamment les conventions de dénomination, les signatures de gestionnaire valides et les bonnes pratiques. Cette page inclut également un exemple de fonction d'événement Lambda en Python qui collecte des informations sur une commande, produit un reçu sous forme de fichier texte et place ce fichier dans un bucket Amazon Simple Storage Service (Amazon S3).

Rubriques

- Exemple de code de fonction d'événement Lambda en Python
- Convention de nommage du gestionnaire
- Utilisation de l'objet d'événement Lambda
- Accès et utilisation de l'objet de contexte Lambda
- Signatures de gestionnaire valides pour les gestionnaires Python
- Renvoi d'une valeur
- Utilisation de AWS SDK pour Python (Boto3) dans votre gestionnaire
- Accès aux variables d'environnement
- Meilleures pratiques en matière de code pour les fonctions d'événement Lambda en Python

Exemple de code de fonction d'événement Lambda en Python

L'exemple de code de fonction Lambda Python suivant prend en compte les informations relatives à une commande, produit un reçu sous forme de fichier texte et place ce fichier dans un compartiment Amazon S3 :

Example Fonction d'événement Lambda en Python

```
import json
import os
import logging
import boto3

# Initialize the S3 client outside of the handler
s3_client = boto3.client('s3')
```

```
# Initialize the logger
logger = logging.getLogger()
logger.setLevel("INFO")

def upload_receipt_to_s3(bucket_name, key, receipt_content):
    """Helper function to upload receipt to S3"""

    try:
        s3_client.put_object(
            Bucket=bucket_name,
            Key=key,
            Body=receipt_content
        )
    except Exception as e:
        logger.error(f"Failed to upload receipt to S3: {str(e)}")
        raise

def lambda_handler(event, context):
    """
    Main Lambda handler function
    Parameters:
        event: Dict containing the Lambda function event data
        context: Lambda runtime context
    Returns:
        Dict containing status message
    """
    try:
        # Parse the input event
        order_id = event['Order_id']
        amount = event['Amount']
        item = event['Item']

        # Access environment variables
        bucket_name = os.environ.get('RECEIPT_BUCKET')
        if not bucket_name:
            raise ValueError("Missing required environment variable RECEIPT_BUCKET")

        # Create the receipt content and key destination
        receipt_content = (
            f"OrderID: {order_id}\n"
            f"Amount: ${amount}\n"
            f"Item: {item}"
        )
```

```
        key = f"receipts/{order_id}.txt"

        # Upload the receipt to S3
        upload_receipt_to_s3(bucket_name, key, receipt_content)

        logger.info(f"Successfully processed order {order_id} and stored receipt in S3
bucket {bucket_name}")

        return {
            "statusCode": 200,
            "message": "Receipt processed successfully"
        }

    except Exception as e:
        logger.error(f"Error processing order: {str(e)}")
        raise
```

Ce fichier comprend les sections suivantes :

- `import`bloc : utilisez ce bloc pour inclure les bibliothèques requises par votre fonction.
- Initialisation globale du client SDK et de l'enregistreur : l'inclusion du code d'initialisation en dehors du gestionnaire permet de tirer parti de la réutilisation de l'environnement d'exécution afin d'améliorer les performances de votre fonction. Pour en savoir plus, consultez the section called "Meilleures pratiques en matière de code pour les fonctions d'événement Lambda en Python".
- `def upload_receipt_to_s3(bucket_name, key, receipt_content):` une fonction d'assistance appelée par la fonction `lambda_handler` principale.
- `def lambda_handler(event, context):` la fonction de gestion principale de votre code, qui contient la logique principale de votre application. Lorsque Lambda invoque votre gestionnaire de fonction, l'environnement d'exécution Lambda transmet deux arguments à la fonction, l'objet d'événement qui contient les données à traiter par votre fonction, et l'objet de contexte qui contient des informations sur l'invocation de la fonction.

Convention de nommage du gestionnaire

Le nom du gestionnaire de fonctions défini au moment de la création d'une fonction est dérivé de :

- Nom du fichier dans lequel se trouve la fonction du gestionnaire Lambda.
- Nom de la fonction du gestionnaire Python.

Dans l'exemple ci-dessus, si le fichier est nommé `lambda_function.py`, le gestionnaire sera spécifié comme `lambda_function.lambda_handler`. Il s'agit du nom de gestionnaire par défaut donné aux fonctions que vous créez avec la console Lambda.

Si vous créez une fonction dans la console en utilisant un nom de fichier ou un nom de gestionnaire de fonction différent, vous devez modifier le nom du gestionnaire par défaut.

Pour modifier le nom du gestionnaire de fonction (console)

1. Ouvrez la page Event Functions de la console Lambda et choisissez votre fonction.
2. Cliquez sur l'onglet Code.
3. Faites défiler l'écran jusqu'au volet Paramètres d'exécution et choisissez Modifier.
4. Dans Gestionnaire, saisissez le nouveau nom de votre gestionnaire de fonction.
5. Cliquez sur Enregistrer.

Utilisation de l'objet d'événement Lambda

Lorsque Lambda invoque votre fonction, il transmet un argument d'objet d'événement au gestionnaire de fonction. Les objets JSON constituent le format d'événement le plus courant pour les fonctions d'événement Lambda. Dans l'exemple de code de la section précédente, la fonction exige une entrée au format suivant :

```
{
    "Order_id": "12345",
    "Amount": 199.99,
    "Item": "Wireless Headphones"
}
```

Si votre fonction est invoquée par un autre Service AWS, l'événement d'entrée est également un objet JSON. Le format exact de l'objet d'événement dépend du service qui invoque votre fonction. Pour connaître le format de l'événement pour un service en particulier, reportez-vous à la page appropriée du chapitre the section called "Intégration d'autres services".

Si l'événement d'entrée est un objet JSON, le moteur d'exécution Lambda le convertit en dictionnaire Python. Pour attribuer des valeurs dans le JSON d'entrée aux variables de votre code, utilisez les méthodes standard des dictionnaires Python, comme illustré dans l'exemple de code.

Vous pouvez également transmettre des données à votre fonction sous forme de tableau JSON ou de n'importe quel autre type de données JSON valide. Le tableau suivant définit la manière dont le moteur d'exécution Python convertit ces types JSON.

Type de données JSON	Type de données Python
objet	dictionnaire (`dict`)
array	liste (`list`)
number	entier (`int`) ou nombre à virgule flottante (`float`)
chaîne	chaîne (`str`)
Booléen	Booléen () `bool`
null	NoneType (`NoneType`)

Accès et utilisation de l'objet de contexte Lambda

L'objet de contexte Lambda contient des informations sur la fonction, l'invocation et l'environnement d'exécution. Lambda transmet automatiquement l'objet de contexte à votre fonction lors de son invocation. Vous pouvez utiliser l'objet de contexte pour générer des informations sur l'invocation de votre fonction à des fins de surveillance.

L'objet de contexte est une classe Python définie dans le client d'interface d'environnement d'exécution Lambda. Pour renvoyer la valeur de l'une des propriétés de l'objet de contexte, utilisez la méthode correspondante sur l'objet de contexte. Par exemple, l'extrait de code suivant attribue la valeur de la propriété `aws_request_id` (l'identifiant de la demande d'invocation) à une variable nommée `request`.

```
request = context.aws_request_id
```

Pour en savoir plus sur l'utilisation de l'objet de contexte Lambda et pour consulter la liste complète des méthodes et propriétés disponibles, consultez the section called "Contexte".

Signatures de gestionnaire valides pour les gestionnaires Python

Lorsque vous définissez votre fonction de gestionnaire en Python, la fonction doit accepter deux arguments. Le premier de ces arguments est l'objet d'événement Lambda, et le second est l'objet de contexte Lambda. Par convention, ces arguments d'entrée sont généralement nommés `event` et `context`, mais vous pouvez leur donner le nom que vous souhaitez. Si vous déclarez votre fonction de gestionnaire avec un seul argument d'entrée, Lambda génère une erreur lorsqu'il tente d'exécuter votre fonction. La méthode la plus courante pour déclarer une fonction de gestionnaire en Python est la suivante :

```
def lambda_handler(event, context):
```

Vous pouvez également utiliser des indications de type Python dans votre déclaration de fonction, comme illustré dans l'exemple suivant :

```
from typing import Dict, Any

def lambda_handler(event: Dict[str, Any], context: Any) -> Dict[str, Any]:
```

Pour utiliser une AWS saisie spécifique pour les événements générés par d'autres Services AWS et pour l'objet de contexte, ajoutez le `aws-lambda-typing` package au package de déploiement de votre fonction. Vous pouvez installer cette bibliothèque dans votre environnement de développement en exécutant **`pip install aws-lambda-typing`**. L'extrait de code suivant montre comment utiliser les indices de type AWS spécifiques. Dans cet exemple, l'événement attendu est un événement Amazon S3.

```
from aws_lambda_typing.events import S3Event
from aws_lambda_typing.context import Context
from typing import Dict, Any

def lambda_handler(event: S3Event, context: Context) -> Dict[str, Any]:
```

Vous ne pouvez pas utiliser le type de fonction `async` Python pour votre fonction de gestionnaire.

Renvoi d'une valeur

Un gestionnaire peut renvoyer une valeur, qui doit être sérialisable en JSON. Les types de retour les plus courants comprennent `dict`, `list`, `str`, `int`, `float` et `bool`.

Ce qu'il advient de la valeur renvoyée dépend du type d'invocation et du service qui a invoqué la fonction. Par exemple :

- Si vous utilisez le type d'`RequestResponse`invocation pour appeler une fonction de manière synchrone, Lambda renvoie le résultat de l'appel de fonction Python au client qui appelle la fonction (dans la réponse HTTP à la demande d'appel, sérialisée en JSON). Par exemple, la AWS Lambda console utilise le type d'`RequestResponse`invocation. Ainsi, lorsque vous appelez la fonction sur la console, la console affiche la valeur renvoyée.
- Si le gestionnaire renvoie des objets qui ne peuvent pas être sérialisées par `json.dumps`, le runtime renvoie une erreur. Il existe une exception à cette règle si le gestionnaire renvoie un `bytes` objet.
- Si le gestionnaire renvoie un `bytes` objet, le moteur d'exécution le transmet tel quel sous forme de données binaires brutes sans sérialisation JSON, en utilisant un type de contenu de. `application/unknown`
- Si le gestionnaire renvoie `None`, comme le font implicitement les fonctions Python sans une instruction `return`, le runtime renvoie `null`.
- Si vous exécutez le type d'invocation `Event` (une invocation asynchrone), la valeur sera ignorée.

Dans l'exemple de code, le gestionnaire renvoie le dictionnaire Python suivant :

```
{
  "statusCode": 200,
  "message": "Receipt processed successfully"
}
```

L'environnement d'exécution Lambda sérialise ce dictionnaire et le renvoie au client qui a invoqué la fonction sous forme de chaîne JSON.

> **Note**
>
> Dans Python 3.9 et les versions ultérieures, Lambda inclut le requestId de l'invocation dans la réponse d'erreur.

Utilisation de AWS SDK pour Python (Boto3) dans votre gestionnaire

Souvent, vous utiliserez vos fonctions pour interagir avec Services AWS d'autres ressources. Le moyen le plus simple d'interagir avec ces ressources est d'utiliser AWS SDK pour Python (Boto3). Tous les environnements d'exécution Lambda Python pris en charge incluent une version du SDK pour Python (Boto3).

Toutefois, nous vous recommandons vivement d'inclure le SDK dans le package de déploiement de votre fonction si votre code doit l'utiliser. L'inclusion du SDK dans votre package de déploiement vous permet de contrôler totalement vos dépendances et de réduire le risque de problèmes d'incompatibilité des versions avec les autres bibliothèques. Pour en savoir plus, consultez the section called "Dépendances d'exécution dans Python" et the section called "Rétrocompatibilité".

Pour utiliser le SDK pour Python (Boto3) dans votre fonction, ajoutez l'instruction suivante au bloc d'importation au début du code de votre fonction :

```
import boto3
```

Utilisez la commande `pip install` pour ajouter la bibliothèque `boto3` au package de déploiement de votre fonction. Pour des instructions détaillées sur l'ajout de dépendances à un package de déploiement .zip, consultez the section called "Création d'un package de déploiement .zip avec dépendances". Pour en savoir plus sur l'ajout de dépendances aux fonctions déployées sous forme d'images de conteneur, consultez the section called "Création d'une image à partir d'une image de base" outhe section called "Création d'une image à partir d'une image de base alternative".

Lorsque vous utilisez `boto3` dans votre code, vous n'avez pas besoin de fournir des informations d'identification pour initialiser un client. Par exemple, dans l'exemple de code, nous utilisons la ligne de code suivante pour initialiser un client Amazon S3 :

```
# Initialize the S3 client outside of the handler
s3_client = boto3.client('s3')
```

Avec Python, Lambda crée automatiquement des variables d'environnement avec des informations d'identification. Le SDK `boto3` vérifie la présence de ces informations d'identification dans les variables d'environnement de votre fonction lors de l'initialisation.

Accès aux variables d'environnement

Dans le code de votre gestionnaire, vous pouvez référencer les variables d'environnement à l'aide de la méthode `os.environ.get`. Dans l'exemple de code, nous référençons la variable d'environnement `RECEIPT_BUCKET` définie à l'aide de la ligne de code suivante :

```
# Access environment variables
bucket_name = os.environ.get('RECEIPT_BUCKET')
```

N'oubliez pas d'inclure une instruction `import os` dans le bloc import au début de votre code.

Meilleures pratiques en matière de code pour les fonctions d'événement Lambda en Python

Respectez les directives de la liste suivante pour utiliser les meilleures pratiques de codage lors de la création de vos fonctions :

- Séparez le gestionnaire Lambda de votre logique principale. Cela facilite la création d'une fonction plus testable à l'unité. Par exemple, en Python, cela peut ressembler à ceci :

  ```
  def lambda_handler(event, context):
      foo = event['foo']
      bar = event['bar']
      result = my_lambda_function(foo, bar)

  def my_lambda_function(foo, bar):
      // MyLambdaFunction logic here
  ```

- Contrôlez les dépendances dans le package de déploiement de votre fonction. L'environnement d'exécution AWS Lambda contient un certain nombre de bibliothèques. Pour les Node.js environnements d'exécution et Python, ceux-ci incluent les AWS SDK.

  Pour activer les dernières fonctionnalités et mises à jour de sécurité, Lambda met régulièrement à jour ces bibliothèques. Ces mises à jour peuvent apporter des modifications subtiles au comportement de votre fonction. Pour disposer du contrôle total des dépendances que votre fonction utilise, empaquetez toutes vos dépendances avec votre package de déploiement.
- Réduisez la complexité de vos dépendances. Privilégiez les infrastructures plus simples qui se chargent rapidement au démarrage de l'environnement d'exécution.
- Réduisez la taille de votre package de déploiement selon ses besoins d'exécution. Cela réduit le temps nécessaire au téléchargement et au déballage de votre package de déploiement avant l'invocation.

Tirez parti de la réutilisation de l'environnement d'exécution pour améliorer les performances de votre fonction. Initialisez les clients SDK et les connexions à la base de données en dehors du gestionnaire de fonctions et mettez en cache les actifs statiques localement dans le répertoire `/tmp`. Les invocations ultérieures traitées par la même instance de votre fonction peuvent réutiliser ces ressources. Cela permet d'économiser des coûts, tout en réduisant le temps d'exécution de la fonction.

Pour éviter des éventuelles fuites de données entre les invocations, n'utilisez pas l'environnement d'exécution pour stocker des données utilisateur, des événements ou d'autres informations ayant un impact sur la sécurité. Si votre fonction repose sur un état réversible qui ne peut pas être stocké en mémoire dans le gestionnaire, envisagez de créer une fonction distincte ou des versions distinctes d'une fonction pour chaque utilisateur.

Utilisez une directive keep-alive pour maintenir les connexions persistantes. Lambda purge les connexions inactives au fil du temps. Si vous tentez de réutiliser une connexion inactive lorsque vous invoquez une fonction, cela entraîne une erreur de connexion. Pour maintenir votre connexion persistante, utilisez la directive Keep-alive associée à votre environnement d'exécution. Pour un exemple, voir Réutilisation des connexions avec Keep-Alive in Node.js.

Utilisez des variables d'environnement pour transmettre des paramètres opérationnels à votre fonction. Par exemple, si vous écrivez dans un compartiment Amazon S3 au lieu de coder en dur le nom du compartiment dans lequel vous écrivez, configurez le nom du compartiment comme variable d'environnement.

Évitez d'utiliser des invocations récursives dans votre fonction Lambda, lorsque la fonction s'invoque elle-même ou démarre un processus susceptible de l'invoquer à nouveau. Cela peut entraîner un volume involontaire d'invocations de fonction et des coûts accrus. Si vous constatez un volume involontaire d'invocations, définissez immédiatement la simultanéité réservée à la fonction sur `0` afin de limiter toutes les invocations de la fonction, pendant que vous mettez à jour le code.

N'utilisez pas d'API non publiques non documentées dans le code de votre fonction Lambda. Pour les AWS Lambda environnements d'exécution gérés, Lambda applique régulièrement des mises à jour fonctionnelles et de sécurité aux API internes de Lambda. Ces mises à jour internes de l'API peuvent être incompatibles avec les versions antérieures, entraînant des conséquences imprévues telles que des échecs d'invocation si votre fonction dépend de ces API non publiques. Consultez la Référence d'API pour obtenir la liste des API accessibles au public.

Écriture du code idempotent. L'écriture de code idempotent pour vos fonctions garantit ne gestion identique des événements dupliqués. Votre code doit valider correctement les événements

et gérer correctement les événements dupliqués. Pour de plus amples informations, veuillez consulterComment faire en sorte que ma fonction Lambda soit idempotente ?.

Utilisation d'archives de fichiers .zip pour les fonctions événementielles Lambda en Python

Le code de votre AWS Lambda fonction comprend un fichier .py contenant le code du gestionnaire de votre fonction, ainsi que les packages et modules supplémentaires dont dépend votre code. Pour déployer ce code de fonction vers Lambda, vous utilisez un package de déploiement. Ce package peut être une archive de fichier .zip ou une image de conteneur. Pour plus d'informations sur l'utilisation d'images de conteneur avec Python, voir Déployer des fonctions d'événement Lambda en Python avec des images de conteneur.

Pour créer votre package de déploiement sous forme d'archive de fichier .zip, vous pouvez utiliser l'utilitaire d'archivage .zip intégré à votre outil de ligne de commande, ou tout autre utilitaire .zip tel que 7zip. Les exemples présentés dans les sections suivantes supposent que vous utilisez un outil `zip` de ligne de commande dans un environnement Linux ou macOS. Pour utiliser les mêmes commandes sous Windows, vous pouvez installer le sous-système Windows pour Linux afin d'obtenir une Windows-integrated version d'Ubuntu et de Bash.

Notez que Lambda utilise les autorisations de fichiers POSIX. Ainsi, vous pourriez devoir définir des autorisations pour le dossier du package de déploiement avant de créer l'archive de fichiers .zip.

Rubriques

- Dépendances d'exécution dans Python
- Création d'un package de déploiement .zip sans dépendances
- Création d'un package de déploiement .zip avec dépendances
- Chemin de recherche des dépendances et bibliothèques incluses dans l'exécution
- Utilisation des dossiers __pycache__
- Création de packages de déploiement .zip avec des bibliothèques natives
- Création et mise à jour de fonctions d'événements Lambda en Python à l'aide de fichiers .zip

Dépendances d'exécution dans Python

Pour les fonctions d'événement Lambda qui utilisent l'environnement d'exécution Python, une dépendance peut être n'importe quel package ou module Python. Lorsque vous déployez votre fonction à l'aide d'une archive .zip, vous pouvez soit ajouter ces dépendances à votre fichier .zip avec votre code de fonction, soit utiliser une couche Lambda. Une couche est un fichier .zip séparé qui peut contenir du code supplémentaire et d'autres contenus. Pour en savoir plus sur l'utilisation des couches Lambda dans Python, consultez the section called "Layers".

Les environnements d'exécution Lambda Python incluent le AWS SDK pour Python (Boto3) et ses dépendances. Lambda fournit le kit SDK dans l'environnement d'exécution pour les scénarios de déploiement où vous n'êtes pas en mesure d'ajouter vos propres dépendances. Ces scénarios incluent la création de fonctions dans la console à l'aide de l'éditeur de code intégré ou à l'utilisation de fonctions intégrées dans AWS Serverless Application Model (AWS SAM) ou de CloudFormation modèles.

Lambda met régulièrement à jour les bibliothèques d'exécution Python afin d'inclure les dernières mises à jour et correctifs de sécurité. Si votre fonction utilise la version du kit SDK Boto3 incluse dans l'exécution, mais que votre package de déploiement inclut des dépendances du kit SDK, cela peut entraîner des problèmes d'alignement de versions. Par exemple, votre package de déploiement peut inclure la dépendance du kit SDK urllib3. Lorsque Lambda met à jour le kit SDK dans l'exécution, des problèmes de compatibilité entre la nouvelle version de l'exécution et la version d'urllib3 de votre package de déploiement peuvent faire échouer votre fonction.

> **Important**
>
> Pour conserver un contrôle total sur vos dépendances et éviter d'éventuels problèmes de désalignement des versions, nous vous recommandons d'ajouter toutes les dépendances de votre fonction à votre package de déploiement, même si des versions de celles-ci sont incluses dans le runtime Lambda. Cela inclut le kit SDK Boto3.

Pour savoir quelle version du kit SDK pour Python (Boto3) est incluse dans l'environnement d'exécution que vous utilisez, consultez the section called "Runtime-included Versions du SDK".

Dans le cadre du modèle de responsabilité partagée AWS, vous êtes responsable de la gestion de toutes les dépendances dans les packages de déploiement de vos fonctions. Cela inclut l'application de mises à jour et de correctifs de sécurité. Pour mettre à jour les dépendances dans le package de déploiement de votre fonction, créez d'abord un nouveau fichier .zip, puis chargez-le sur Lambda. Pour plus d'informations, consultez Création d'un package de déploiement .zip avec dépendances et Création et mise à jour de fonctions d'événements Lambda en Python à l'aide de fichiers .zip.

Création d'un package de déploiement .zip sans dépendances

Si le code de votre fonction ne comporte aucune dépendance, votre fichier .zip contient uniquement le fichier .py contenant le code du gestionnaire de votre fonction. Utilisez votre utilitaire zip préféré pour créer un fichier .zip avec votre fichier .py à la racine. Si le fichier .py ne se trouve pas à la racine de votre fichier .zip, Lambda ne pourra pas exécuter votre code.

Pour savoir comment déployer votre fichier .zip afin de créer une nouvelle fonction ou de mettre à jour une fonction existante, consultezCréation et mise à jour de fonctions d'événements Lambda en Python à l'aide de fichiers .zip.

Création d'un package de déploiement .zip avec dépendances

Si votre code de fonction dépend de packages ou de modules supplémentaires, vous pouvez soit ajouter ces dépendances à votre fichier .zip avec votre code de fonction, soit utiliser une couche Lambda. Les instructions de cette section vous indiquent comment inclure vos dépendances dans votre package de déploiement .zip. Pour que Lambda puisse exécuter votre code, le fichier .py contenant le code de votre gestionnaire et toutes les dépendances de votre fonction doit être installé à la racine du fichier .zip.

Supposons que votre code de fonction soit enregistré dans un fichier nommé `lambda_function.py`. L'exemple de commandes d'interface de ligne de commande suivant crée un fichier .zip nommé `my_deployment_package.zip` contenant le code de votre fonction et ses dépendances. Vous pouvez soit installer vos dépendances directement dans un dossier du répertoire de votre projet, soit utiliser un environnement virtuel Python.

Pour créer le package de déploiement (répertoire du projet)

1. Accédez au répertoire du projet qui contient votre fichier de code source `lambda_function.py`. Dans cet exemple, le répertoire est nommé `my_function`.

   ```
   cd my_function
   ```

2. Créez un nouveau répertoire nommé « package » dans lequel vous installerez vos dépendances.

   ```
   mkdir package
   ```

   Notez que pour un package de déploiement .zip, Lambda s'attend à ce que votre code source et ses dépendances se trouvent tous à la racine du fichier .zip. Toutefois, l'installation de dépendances directement dans le répertoire de votre projet peut introduire un grand nombre de nouveaux fichiers et dossiers et rendre la navigation dans votre IDE difficile. Vous créez ici un répertoire `package` distinct pour séparer vos dépendances de votre code source.

3. Installez les dépendances dans le répertoire `package`. L'exemple ci-dessous installe le kit SDK Boto3 à partir de l'index du Python Package Index à l'aide de pip. Si le code de votre fonction

utilise des packages Python que vous avez créés vous-même, enregistrez-les dans le répertoire `package`.

```
pip install --target ./package boto3
```

4. Créez un fichier .zip avec les bibliothèques installées à la racine.

```
cd package
zip -r ../my_deployment_package.zip .
```

Cela génère un fichier `my_deployment_package.zip` dans votre répertoire de projet.

5. Ajoutez le fichier lambda_function.py à la racine du fichier .zip.

```
cd ..
zip my_deployment_package.zip lambda_function.py
```

Votre fichier .zip doit avoir une structure de répertoires horizontale, avec le code du gestionnaire de votre fonction et tous vos dossiers de dépendances installés à la racine comme suit.

```
my_deployment_package.zip
|- bin
|  |-jp.py
|- boto3
|  |-compat.py
|  |-data
|  |-docs
...
|- lambda_function.py
```

Si le fichier .py contenant le code du gestionnaire de votre fonction ne se trouve pas à la racine de votre fichier .zip, Lambda ne peut pas exécuter votre code.

Pour créer le package de déploiement (environnement virtuel)

1. Créez et activez un environnement virtuel dans le répertoire de votre projet. Dans cet exemple, le répertoire du projet est nommé `my_function`.

```
~$ cd my_function
~/my_function$ python3.14 -m venv my_virtual_env
```

```
~/my_function$ source ./my_virtual_env/bin/activate
```

2. Installez les bibliothèques requises à l'aide de pip. L'exemple suivant permet d'installer le kit SDK Boto3

```
(my_virtual_env) ~/my_function$ pip install boto3
```

3. Utilisez `pip show` pour trouver l'emplacement dans votre environnement virtuel où pip a installé vos dépendances.

```
(my_virtual_env) ~/my_function$ pip show <package_name>
```

Le dossier dans lequel pip installe vos bibliothèques peut être nommé `site-packages` ou. `dist-packages` Ce dossier peut se trouver dans le `lib64/python3.x` répertoire `lib/python3.x` or (où python3.x représente la version de Python que vous utilisez).

4. Désactivation de l'environnement virtuel

```
(my_virtual_env) ~/my_function$ deactivate
```

5. Accédez au répertoire contenant les dépendances que vous avez installées avec pip et créez un fichier .zip dans le répertoire de votre projet avec les dépendances installées à la racine. Dans cet exemple, pip a installé vos dépendances dans le répertoire `my_virtual_env/lib/python3.14/site-packages`.

```
~/my_function$ cd my_virtual_env/lib/python3.14/site-packages
~/my_function/my_virtual_env/lib/python3.14/site-packages$ zip -r ../../../../
my_deployment_package.zip .
```

6. Accédez à la racine du répertoire de votre projet où se trouve le fichier .py contenant le code de votre gestionnaire et ajoutez ce fichier à la racine de votre package .zip. Dans cet exemple, votre fichier de code de fonction est nommé `lambda_function.py`.

```
~/my_function/my_virtual_env/lib/python3.14/site-packages$ cd ../../../../
~/my_function$ zip my_deployment_package.zip lambda_function.py
```

Chemin de recherche des dépendances et bibliothèques incluses dans l'exécution

Lorsque vous utilisez une instruction `import` dans votre code, l'exécution Python recherche les répertoires dans son chemin de recherche jusqu'à ce qu'elle trouve le module ou le package. Par

défaut, le premier emplacement dans lequel recherche l'exécution est le répertoire dans lequel votre package de déploiement .zip est décompressé et monté (`/var/task`). Si vous incluez une version d'une bibliothèque incluse dans l'environnement d'exécution dans votre package de déploiement, votre version a priorité sur la version incluse dans le moteur d'exécution. Les dépendances de votre package de déploiement ont également la priorité sur les dépendances des couches.

Lorsque vous ajoutez une dépendance à une couche, Lambda l'extrait vers `/opt/python/lib/python3.x/site-packages` (où `python3.x` représente la version de l'exécution que vous utilisez) ou `/opt/python`. Dans le chemin de recherche, ces répertoires ont la priorité sur les répertoires contenant les bibliothèques incluses dans l'exécution et les bibliothèques installées par pip (`/var/runtime` et `/var/lang/lib/python3.x/site-packages`). Les bibliothèques des couches de fonctions ont donc la priorité sur les versions incluses dans l'exécution.

> **Note**
>
> Dans le runtime géré et l'image de base de Python 3.11, le AWS SDK et ses dépendances sont installés dans le `/var/lang/lib/python3.11/site-packages` répertoire.

Vous pouvez consulter le chemin de recherche complet de votre fonction en ajoutant l'extrait de code suivant.

```
import sys

search_path = sys.path
print(search_path)
```

> **Note**
>
> Étant donné que les dépendances de votre package de déploiement ou de vos couches sont prioritaires sur les bibliothèques incluses dans l'exécution, cela peut entraîner des problèmes d'alignement de versions si vous incluez une dépendance du kit SDK telle que urllib3 dans votre package sans inclure également le kit SDK. Si vous déployez votre propre version d'une dépendance de Boto3, vous devez également déployer Boto3 en tant que dépendance dans votre package de déploiement. Nous vous recommandons de créer un package pour toutes les dépendances de votre fonction, même si des versions de celles-ci sont incluses dans le runtime.

Vous pouvez également ajouter des dépendances dans un dossier distinct au sein de votre package .zip. Par exemple, vous pouvez ajouter une version du kit SDK Boto3 dans un dossier de votre package .zip appelé `common`. Lorsque votre package .zip est décompressé et monté, ce dossier est placé dans le répertoire `/var/task`. Pour utiliser dans votre code une dépendance provenant d'un dossier de votre package de déploiement .zip, utilisez une instruction `import from`. Par exemple, pour utiliser une version de Boto3 provenant d'un dossier nommé `common` dans votre package .zip, utilisez l'instruction suivante.

```
from common import boto3
```

Utilisation des dossiers __pycache__

Nous vous recommandons de ne pas inclure de dossiers `__pycache__` dans le package de déploiement de votre fonction. Le bytecode Python compilé sur une machine de génération avec une architecture ou un système d'exploitation différent peut ne pas être compatible avec l'environnement d'exécution Lambda.

Création de packages de déploiement .zip avec des bibliothèques natives

Si votre fonction utilise uniquement des packages et des modules Python purs, vous pouvez utiliser la commande `pip install` pour installer vos dépendances sur n'importe quelle machine de génération locale et créer votre fichier .zip. De nombreuses bibliothèques Python populaires, y compris NumPy Pandas, ne sont pas du Python pur et contiennent du code écrit en C ou C++. Lorsque vous ajoutez des bibliothèques contenant du code C/C ++ à votre package de déploiement, vous devez créer votre package correctement pour garantir sa compatibilité avec l'environnement d'exécution Lambda.

La plupart des packages disponibles sur le Python Package Index (PyPI) sont disponibles sous forme de « roues » (fichiers .whl). Un fichier .whl est un type de fichier ZIP qui contient une distribution intégrée avec des fichiers binaires précompilés pour un système d'exploitation et une architecture de l'ensemble des instructions particuliers. Pour rendre votre package de déploiement compatible avec Lambda, vous devez installer la roue pour les systèmes d'exploitation Linux et l'architecture du jeu d'instructions de votre fonction.

Certains packages peuvent uniquement être disponibles en tant que distributions sources. Pour ces packages, vous devez compiler et construire vous-même les composants C/C ++.

Pour connaître les distributions disponibles pour le package dont vous avez besoin, procédez comme suit :

1. Recherchez le nom du package sur la page principale du Python Package Index.
2. Choisissez la version du package que vous souhaitez utiliser.
3. Choisissez Télécharger les fichiers.

Utilisation des distributions intégrées (fichiers wheels)

Pour télécharger une roue compatible avec Lambda, utilisez l'option `--platform` pip.

Si votre fonction utilise l'architecture du jeu d'instructions x86_64, exécutez la `pip install` commande suivante pour installer une roue compatible dans votre répertoire. `package` Remplacez `--python 3.x` par la version d'exécution Python que vous utilisez.

```
pip install \
--platform manylinux2014_x86_64 \
--target=package \
--implementation cp \
--python-version 3.x \
--only-binary=:all: --upgrade \
<package_name>
```

Si votre fonction utilise l'architecture de l'ensemble d'instructions arm64, exécutez la commande suivante. Remplacez `--python 3.x` par la version d'exécution Python que vous utilisez.

```
pip install \
--platform manylinux2014_aarch64 \
--target=package \
--implementation cp \
--python-version 3.x \
--only-binary=:all: --upgrade \
<package_name>
```

Utilisation des distributions sources

Si votre package n'est disponible qu'en tant que distribution source, vous devez créer vous-même les bibliothèques C/C ++. Pour rendre votre package compatible avec l'environnement d'exécution Lambda, vous devez le créer dans un environnement qui utilise le même système d'exploitation Amazon Linux. Pour ce faire, créez votre package dans une instance Amazon Elastic Compute Cloud (Amazon EC2) Linux.

Pour savoir comment lancer une instance Amazon EC2 Linux et s'y connecter, veuillez consulter Mise en route avec Amazon EC2 dans le Guide de l'utilisateur Amazon EC2.

Création et mise à jour de fonctions d'événements Lambda en Python à l'aide de fichiers .zip

Une fois que vous avez créé votre package de déploiement .zip, vous pouvez l'utiliser pour créer une nouvelle fonction Lambda ou mettre à jour une fonction Lambda existante. Vous pouvez déployer votre package .zip à l'aide de la console Lambda, de l'API Lambda et AWS Command Line Interface de l'API Lambda. Vous pouvez également créer et mettre à jour des fonctions Lambda à l'aide de l' AWS Serverless Application Model (AWS SAM) et de CloudFormation.

La taille maximale d'un package de déploiement .zip pour Lambda est de 250 Mo (décompressé). Notez que cette limite s'applique à la taille combinée de tous les fichiers que vous chargez, y compris les couches Lambda.

Le runtime Lambda a besoin d'une autorisation pour lire les fichiers de votre package de déploiement. Dans la notation octale des autorisations Linux, Lambda a besoin de 644 autorisations pour les fichiers non exécutables (rw-r--r--) et de 755 autorisations (rwxr-xr-x) pour les répertoires et les fichiers exécutables.

Sous Linux et macOS, utilisez la commande `chmod` pour modifier les autorisations de fichiers sur les fichiers et les répertoires de votre package de déploiement. Par exemple, pour octroyer à un fichier non exécutable les autorisations correctes, exécutez la commande suivante.

```
chmod 644 <filepath>
```

Pour modifier les autorisations relatives aux fichiers dans Windows, voir Définir, afficher, modifier ou supprimer des autorisations sur un objet dans la documentation Microsoft Windows.

> **Note**
>
> Si vous n'octroyez pas à Lambda les autorisations dont il a besoin pour accéder aux répertoires de votre package de déploiement, Lambda définit les autorisations de ces répertoires à 755 (rwxr-xr-x).

Création et mise à jour de fonctions avec des fichiers .zip à l'aide de la console

Pour créer une nouvelle fonction, vous devez d'abord créer la fonction dans la console, puis charger votre archive .zip. Pour mettre à jour une fonction existante, ouvrez la page de votre fonction, puis suivez la même procédure pour ajouter votre fichier .zip mis à jour.

Si votre fichier .zip fait moins de 50 Mo, vous pouvez créer ou mettre à jour une fonction en chargeant le fichier directement à partir de votre ordinateur local. Pour les fichiers .zip de plus de 50 Mo, vous devez d'abord charger votre package dans un compartiment Amazon S3. Pour savoir comment charger un fichier dans un compartiment Amazon S3 à l'aide du Console de gestion AWS, consultez Getting started with Amazon S3. Pour télécharger des fichiers à l'aide de AWS CLI, voir Déplacer des objets dans le guide de AWS CLI l'utilisateur.

> **Note**
>
> Vous ne pouvez pas modifier le type de package de déploiement (.zip ou image de conteneur) d'une fonction existante. Par exemple, vous ne pouvez pas convertir une fonction d'image de conteneur pour utiliser un fichier d'archive .zip à la place. Vous devez créer une nouvelle fonction.

Pour créer une nouvelle fonction (console)

1. Ouvrez la page Event Functions de la console Lambda et choisissez Create Event Function.
2. Choisissez Créer à partir de zéro.
3. Sous Informations de base, procédez comme suit :
   a. Pour Nom de la fonction, saisissez le nom de la fonction.
   b. Pour Exécution, sélectionnez l'exécution que vous souhaitez utiliser.
   c. (Facultatif) Pour Architecture, choisissez l'architecture de l'ensemble des instructions pour votre fonction. L'architecture par défaut est x86_64. Assurez-vous que le package de déploiement .zip pour votre fonction est compatible avec l'architecture de l'ensemble d'instructions que vous sélectionnez.
4. (Facultatif) Sous Permissions (Autorisations), développez Change default execution role (Modifier le rôle d'exécution par défaut). Vous pouvez créer un rôle d'exécution ou en utiliser un existant.

5. Choisissez Create Event Function. Lambda crée une fonction de base « Hello world » à l'aide de l'exécution de votre choix.

Pour charger une archive .zip à partir de votre ordinateur local (console)

1. Sur la page Event Functions de la console Lambda, choisissez la fonction pour laquelle vous souhaitez télécharger le fichier .zip.
2. Sélectionnez l'onglet Code.
3. Dans le volet Source du code, choisissez Charger à partir de.
4. Choisissez Fichier .zip.
5. Pour charger un fichier .zip, procédez comme suit :
   a. Sélectionnez Charger, puis choisissez votre fichier .zip dans le sélecteur de fichiers.
   b. Choisissez Ouvrir.
   c. Cliquez sur Enregistrer.

Pour charger une archive .zip depuis un compartiment Amazon S3 (console)

1. Sur la page Event Functions de la console Lambda, choisissez la fonction pour laquelle vous souhaitez télécharger un nouveau fichier .zip.
2. Sélectionnez l'onglet Code.
3. Dans le volet Source du code, choisissez Charger à partir de.
4. Choisissez l'emplacement Amazon S3.
5. Collez l'URL du lien Amazon S3 de votre fichier .zip et choisissez Enregistrer.

Mise à jour des fonctions du fichier .zip à l'aide de l'éditeur de code de la console

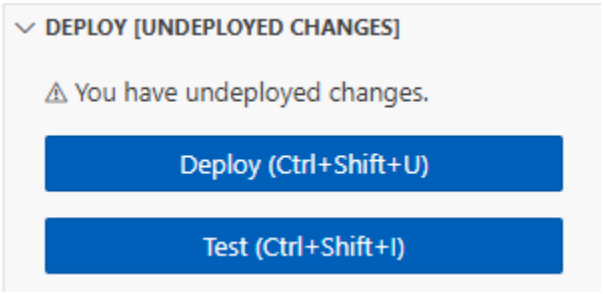
Pour certaines fonctions avec des packages de déploiement .zip, vous pouvez utiliser l'éditeur de code intégré de la console Lambda pour mettre à jour le code de votre fonction directement. Pour utiliser cette fonctionnalité, votre fonction doit répondre aux critères suivants :

- Votre fonction doit utiliser l'un des environnements d'exécution du langage interprété (Python ou Ruby) Node.js
- La taille du package de déploiement de votre fonction doit être inférieure à 50 Mo (décompressé).

Le code des fonctions avec les packages de déploiement d'images de conteneurs ne peut pas être édité directement dans la console.

Pour mettre à jour le code de fonction à l'aide de l'éditeur de code de la console

1. Ouvrez la page Event Functions de la console Lambda et sélectionnez votre fonction.
2. Sélectionnez l'onglet Code.
3. Dans le volet Source du code, sélectionnez votre fichier de code source et modifiez-le dans l'éditeur de code intégré.
4. Dans la section DÉPLOYER, choisissez Déployer pour mettre à jour le code de votre fonction :



Création et mise à jour de fonctions avec des fichiers .zip à l'aide du AWS CLI

Vous pouvez utiliser l'AWS CLI pour créer une nouvelle fonction ou pour mettre à jour une fonction existante à l'aide d'un fichier .zip. Utilisez les commandes create-function et update-function-code pour déployer votre package .zip. Si votre fichier .zip est inférieur à 50 Mo, vous pouvez charger le package .zip à partir d'un emplacement de fichier sur votre machine de génération locale. Pour les fichiers plus volumineux, vous devez charger votre package .zip à partir d'un compartiment Amazon S3. Pour savoir comment charger un fichier dans un compartiment Amazon S3 à l'aide du AWS CLI, consultez la section Déplacer des objets dans le guide de AWS CLI l'utilisateur.

> **Note**
>
> Si vous chargez votre fichier .zip depuis un compartiment Amazon S3 à l'aide de AWS CLI, le compartiment doit se trouver au même endroit Région AWS que votre fonction.

Pour créer une nouvelle fonction à l'aide d'un fichier .zip avec le AWS CLI, vous devez spécifier les éléments suivants :

- Le nom de votre fonction (`--function-name`)

- L'exécution de votre fonction (`--runtime`)
- L'Amazon Resource Name (ARN) du rôle d'exécution de votre fonction (`--role`)
- Le nom de la méthode du gestionnaire dans votre code de fonction (`--handler`)

Vous devez également indiquer l'emplacement de votre fichier .zip. Si votre fichier .zip se trouve dans un dossier sur votre machine de génération locale, utilisez l'option `--zip-file` pour spécifier le chemin d'accès du fichier, comme le montre l'exemple de commande suivant.

```
aws lambda create-function --function-name myFunction \
--runtime python3.14 --handler lambda_function.lambda_handler \
--role arn:aws:iam::111122223333:role/service-role/my-lambda-role \
--zip-file fileb://myFunction.zip
```

Pour spécifier l'emplacement du fichier .zip dans un compartiment Amazon S3, utilisez l'option `--code` comme le montre l'exemple de commande suivant. Vous devez uniquement utiliser le paramètre `S3ObjectVersion` pour les objets soumis à la gestion des versions.

```
aws lambda create-function --function-name myFunction \
--runtime python3.14 --handler lambda_function.lambda_handler \
--role arn:aws:iam::111122223333:role/service-role/my-lambda-role \
--code S3Bucket=amzn-s3-demo-
bucket,S3Key=myFileName.zip,S3ObjectVersion=myObjectVersion
```

Pour mettre à jour une fonction existante à l'aide de l'interface de ligne de commande, vous devez spécifier le nom de votre fonction à l'aide du paramètre `--function-name`. Vous devez également spécifier l'emplacement du fichier .zip que vous souhaitez utiliser pour mettre à jour votre code de fonction. Si votre fichier .zip se trouve dans un dossier sur votre machine de génération locale, utilisez l'option `--zip-file` pour spécifier le chemin d'accès du fichier, comme le montre l'exemple de commande suivant.

```
aws lambda update-function-code --function-name myFunction \
--zip-file fileb://myFunction.zip
```

Pour spécifier l'emplacement du fichier .zip dans un compartiment Amazon S3, utilisez les options `--s3-bucket` et `--s3-key` comme le montre l'exemple de commande suivant. Vous devez uniquement utiliser le paramètre `--s3-object-version` pour les objets soumis à la gestion des versions.

```
aws lambda update-function-code --function-name myFunction \
--s3-bucket amzn-s3-demo-bucket --s3-key myFileName.zip --s3-object-version myObject
 Version
```

Création et mise à jour de fonctions avec des fichiers .zip à l'aide de l'API Lambda

Pour créer et mettre à jour des fonctions à l'aide d'une archive de fichiers .zip, utilisez les opérations d'API suivantes :

- CreateFunction
- UpdateFunctionCode

Création et mise à jour de fonctions avec des fichiers .zip à l'aide de AWS SAM

The AWS Serverless Application Model (AWS SAM) est une boîte à outils qui permet de rationaliser le processus de création et d'exécution d'applications sans serveur sur AWS. Vous définissez les ressources de votre application dans un modèle YAML ou JSON et vous utilisez l'interface de ligne de AWS SAM commande (AWS SAM CLI) pour créer, empaqueter et déployer vos applications. Lorsque vous créez une fonction Lambda à partir d'un AWS SAM modèle, elle crée AWS SAM automatiquement un package de déploiement ou une image de conteneur .zip avec le code de votre fonction et les dépendances que vous spécifiez. Pour en savoir plus sur l'utilisation des fonctions Lambda AWS SAM pour créer et déployer des fonctions Lambda, consultez Getting started with AWS SAM dans le Guide du AWS Serverless Application Model développeur.

Vous pouvez également l'utiliser AWS SAM pour créer une fonction Lambda à l'aide d'une archive de fichiers .zip existante. Pour créer une fonction Lambda à l'aide de AWS SAM, vous pouvez enregistrer votre fichier .zip dans un compartiment Amazon S3 ou dans un dossier local sur votre machine de génération. Pour savoir comment charger un fichier dans un compartiment Amazon S3 à l'aide du AWS CLI, consultez la section Déplacer des objets dans le guide de AWS CLI l'utilisateur.

Dans votre AWS SAM modèle, la `AWS::Serverless::Function` ressource spécifie votre fonction Lambda. Dans cette ressource, définissez les propriétés suivantes pour créer une fonction à l'aide d'une archive de fichiers .zip :

- `PackageType` : défini sur `Zip`
- `CodeUri`- défini sur l'URI Amazon S3, le chemin d'accès au dossier local ou à l'FunctionCodeobjet du code de fonction
- `Runtime` : défini sur votre exécution choisie

Ainsi AWS SAM, si votre fichier .zip est supérieur à 50 Mo, vous n'avez pas besoin de le télécharger au préalable dans un compartiment Amazon S3. AWS SAM peut télécharger des packages .zip jusqu'à la taille maximale autorisée de 250 Mo (décompressés) à partir d'un emplacement sur votre machine de compilation locale.

Pour en savoir plus sur le déploiement de fonctions à l'aide d'un fichier .zip dans AWS SAM, voir AWS::Serverless::Function dans le manuel du AWS SAM développeur.

Création et mise à jour de fonctions avec des fichiers .zip à l'aide de CloudFormation

Vous pouvez l'utiliser CloudFormation pour créer une fonction Lambda à l'aide d'une archive de fichiers .zip. Pour créer une fonction Lambda à partir d'un fichier .zip, vous devez d'abord charger votre fichier dans un compartiment Amazon S3. Pour savoir comment charger un fichier dans un compartiment Amazon S3 à l'aide du AWS CLI, consultez la section Déplacer des objets dans le guide de AWS CLI l'utilisateur.

Pour les Node.js environnements d'exécution pour Python et Python, vous pouvez également fournir du code source intégré dans votre CloudFormation modèle. CloudFormation crée ensuite un fichier .zip contenant votre code lorsque vous créez votre fonction.

Utilisation d'un fichier .zip existant

Dans votre CloudFormation modèle, la `AWS::Lambda::Function` ressource spécifie votre fonction Lambda. Dans cette ressource, définissez les propriétés suivantes pour créer une fonction à l'aide d'une archive de fichiers .zip :

- `PackageType` : défini sur `Zip`
- `Code` : saisissez le nom du compartiment Amazon S3 et le nom du fichier .zip dans les champs `S3Bucket` et `S3Key`
- `Runtime` : défini sur votre exécution choisie

Création d'un fichier .zip à partir du code en ligne

Vous pouvez déclarer des fonctions simples écrites en Python ou Node.js intégrées dans un CloudFormation modèle. Le code étant intégré dans YAML ou JSON, vous ne pouvez pas ajouter de dépendances externes à votre package de déploiement. Cela signifie que votre fonction doit utiliser la version du AWS SDK incluse dans le runtime. Les exigences du modèle, telles que l'obligation d'échapper certains caractères, rendent également plus difficile l'utilisation des fonctionnalités de vérification syntaxique et de complétion de code de votre IDE. Cela signifie que votre modèle peut

nécessiter des tests supplémentaires. En raison de ces limitations, la déclaration de fonctions en ligne convient mieux à un code très simple qui ne change pas fréquemment.

Pour créer un fichier .zip à partir du code en ligne pour et des environnements d'exécution Node.js Python, définissez les propriétés suivantes dans la ressource de votre modèle : `AWS::Lambda::Function`

- `PackageType` : défini sur `Zip`
- `Code` : saisissez votre code de fonction dans le champ `ZipFile`
- `Runtime` : défini sur votre exécution choisie

Le fichier .zip CloudFormation généré ne peut pas dépasser 4 Mo. Pour en savoir plus sur le déploiement de fonctions à l'aide d'un fichier .zip dans CloudFormation, voir AWS::Lambda::Function dans le guide de l'CloudFormation utilisateur.

Déployer des fonctions d'événement Lambda en Python avec des images de conteneur

Il existe trois méthodes pour créer une image de conteneur pour une fonction d'événement Lambda en Python :

- À l'aide d'un AWS image de base pour Python

  Les images de base AWS sont préchargées avec une exécution du langage, un client d'interface d'exécution pour gérer l'interaction entre Lambda et votre code de fonction, et un émulateur d'interface d'exécution pour les tests locaux.
- À l'aide d'un AWS OS-only image de base

  AWS OS-only les images de base contiennent une distribution Amazon Linux et l'émulateur d'interface d'exécution. Ces images sont couramment utilisées pour créer des images de conteneur pour les langages compilés, tels que Go et Rust, et pour une langue ou une version linguistique pour laquelle Lambda ne fournit pas d'image de base, telle que Node.js 19. Vous pouvez également utiliser des images OS-only de base pour implémenter un environnement d'exécution personnalisé. Pour rendre l'image compatible avec Lambda, vous devez inclure le client d'interface d'exécution pour Python dans l'image.
- Utilisation d'une image non AWS basique

  Vous pouvez utiliser une autre image de base à partir d'un autre registre de conteneur, comme Alpine Linux ou Debian. Vous pouvez également utiliser une image personnalisée créée par votre organisation. Pour rendre l'image compatible avec Lambda, vous devez inclure le client d'interface d'exécution pour Python dans l'image.

> **Tip**
>
> Pour réduire le temps nécessaire à l'activation des fonctions du conteneur Lambda, consultez Utiliser des générations en plusieurs étapes (français non garanti) dans la documentation Docker. Pour créer des images de conteneur efficaces, suivez la section Bonnes pratiques pour l'écriture de Dockerfiles (français non garanti).

Cette page explique comment créer, tester et déployer des images de conteneur pour Lambda.

Rubriques

- AWS images de base pour Python
- À l'aide d'un AWS image de base pour Python
- Utilisation d'une autre image de base avec le client d'interface d'exécution

AWS images de base pour Python

AWS fournit les images de base suivantes pour Python :

Étiquettes	Environnement d'exécution	Système d'exploitation	Dockerfile	Obsolescence
3,15	Python 3.15	Amazon Linux	Dockerfile pour Python 3.15 sur GitHub	Non planifié
3,14	Python 3.14	Amazon Linux	Dockerfile pour Python 3.14 sur GitHub	30 juin 2029
3.13	Python 3.13	Amazon Linux	Dockerfile pour Python 3.13 sur GitHub	30 juin 2029
3,12	Python 3.12	Amazon Linux	Dockerfile pour Python 3.12 sur GitHub	31 octobre 2028
3,11	Python 3.11	Amazon Linux 2	Dockerfile pour Python 3.11 sur GitHub	30 juin 2027
3,10	Python 3.10	Amazon Linux 2	Dockerfile pour Python 3.10 sur GitHub	31 octobre 2026

Référentiel Amazon ECR : gallery.ecr. aws/lambda/python

Les images de base de Python 3.12 et versions ultérieures sont basées sur l'image de conteneur minimale Amazon Linux 2023. Les images de base Python 3.8-3.11 sont basées sur l'image Amazon Linux 2. AL2023-based les images offrent plusieurs avantages par rapport à Amazon Linux 2, notamment un encombrement de déploiement réduit et des versions mises à jour de bibliothèques telles que`glibc`.

AL2023-based les images utilisent `microdnf` (lié par un lien symboliquednf) comme gestionnaire de packages au lieu deyum, qui est le gestionnaire de packages par défaut dans Amazon Linux 2. `microdnf`est une implémentation autonome de. `dnf` Pour obtenir la liste des packages inclus dans les AL2023-based images, reportez-vous aux colonnes Conteneur minimal de la section Comparaison des packages installés sur Amazon Linux 2023 Container Images. Pour plus d'informations sur les différences entre AL2023 et Amazon Linux 2, consultez Introducing the Amazon Linux 2023 runtime for AWS Lambda sur le blog AWS Compute.

> **Note**
>
> Pour exécuter AL2023-based des images localement, y compris avec AWS Serverless Application Model (AWS SAM), vous devez utiliser Docker version 20.10.10 ou ultérieure.

Chemin de recherche des dépendances dans les images de base

Lorsque vous utilisez une instruction `import` dans votre code, l'exécution Python recherche les répertoires dans son chemin de recherche jusqu'à ce qu'elle trouve le module ou le package. Par défaut, l'exécution recherche d'abord dans le répertoire `{LAMBDA_TASK_ROOT}`. Si vous ajoutez une version d'une bibliothèque incluse dans l'exécution dans votre image, votre version aura la priorité sur la version incluse dans l'exécution.

Les autres étapes du chemin de recherche dépendent de la version de l'image de base Lambda pour Python que vous utilisez :

- Python 3.11 et versions ultérieures : Runtime-included les bibliothèques et les bibliothèques installées sur pip sont installées dans le répertoire. `/var/lang/lib/python3.11/site-packages` Ce répertoire a la priorité sur `/var/runtime` dans le chemin de recherche. Vous pouvez remplacer le kit SDK en utilisant pip pour installer une version plus récente. Vous pouvez utiliser pip pour vérifier que le kit SDK inclus dans l''exécution et ses dépendances sont compatibles avec tous les packages que vous installez.
- Python 3.8-3.10 : les Runtime-included bibliothèques sont installées dans le répertoire. `/var/runtime` Pip-installed les bibliothèques sont installées dans le `/var/lang/lib/python3.x/site-packages` répertoire. Le répertoire `/var/runtime` a la priorité sur `/var/lang/lib/python3.x/site-packages` dans le chemin de recherche.

Vous pouvez consulter le chemin de recherche complet de votre fonction en ajoutant l'extrait de code suivant.

```
import sys

search_path = sys.path
print(search_path)
```

À l'aide d'un AWS image de base pour Python

Conditions préalables

Pour exécuter la procédure indiquée dans cette section, vous devez satisfaire aux exigences suivantes :

- AWS CLI version 2
- Docker (version minimale 25.0.0)
- Le plug-in buildx Docker.
- Python

Création d'une image à partir d'une image de base

Pour créer une image de conteneur à partir d'un AWS image de base pour Python

1. Créez un répertoire pour le projet, puis passez à ce répertoire.

   ```
   mkdir example
   cd example
   ```

2. Créez un nouveau fichier appelé `lambda_function.py`. Vous pouvez ajouter l'exemple de code de fonction suivant au fichier pour le tester, ou utiliser le vôtre.

   Example Fonction Python

   ```
   import sys
   def handler(event, context):
       return 'Hello from AWS Lambda using Python' + sys.version + '!'
   ```

3. Créez un nouveau fichier appelé `requirements.txt`. Si vous utilisez l'exemple de code de fonction de l'étape précédente, vous pouvez laisser le fichier vide, car il n'y a pas de dépendances. Sinon, répertoriez chaque bibliothèque requise. Par exemple, voici à quoi votre

fichier `requirements.txt` doit ressembler si votre fonction utilise AWS SDK pour Python (Boto3) :

Example requirements.txt

```
boto3
```

4. Créez un nouveau Dockerfile avec la configuration suivante :

   - Définir la propriété `FROM` sur l'URI de l'image de base.
   - Utilisez la commande COPY pour copier le code de fonction et les dépendances d'`{LAMBDA_TASK_ROOT}`exécution dans une variable d'Lambda-defined environnement.
   - Définir l'argument `CMD` pour le gestionnaire de la fonction Lambda.

   Notez que l'exemple de Dockerfile n'inclut pas d'instruction USER. Lorsque vous déployez une image de conteneur sur Lambda, Lambda définit automatiquement un utilisateur Linux par défaut disposant d'autorisations de moindre privilège. Ceci est différent du comportement standard de Docker qui est défini par défaut par l'utilisateur `root` lorsqu'aucune instruction `USER` n'est fournie.

   Example Dockerfile

```
FROM public.ecr.aws/lambda/python:3.12

# Copy requirements.txt
COPY requirements.txt ${LAMBDA_TASK_ROOT}

# Install the specified packages
RUN pip install -r requirements.txt

# Copy function code
COPY lambda_function.py ${LAMBDA_TASK_ROOT}

# Set the CMD to your handler (could also be done as a parameter override outside
 of the Dockerfile)
CMD [ "lambda_function.handler" ]
```

5. Générez l'image Docker à l'aide de la commande docker build. L'exemple suivant nomme l'image `docker-image` et lui donne la balise `test`. Pour rendre votre image compatible avec Lambda, vous devez utiliser l'option `--provenance=false`.

```
docker buildx build --platform linux/amd64 --provenance=false -t docker-image:test
 .
```

> **Note**
>
> La commande spécifie l'option `--platform linux/amd64` pour garantir la compatibilité de votre conteneur avec l'environnement d'exécution Lambda, quelle que soit l'architecture de votre machine de génération. Si vous avez l'intention de créer une fonction Lambda à l'aide de l'architecture du jeu d'instructions ARM64, veillez à modifier la commande pour utiliser plutôt l'option `--platform linux/arm64`.

(Facultatif) Testez l'image localement

1. Démarrez votre image Docker à l'aide de la commande docker run. Dans cet exemple, `docker-image` est le nom de l'image et `test` est la balise.

   ```
   docker run --platform linux/amd64 -p 9000:8080 docker-image:test
   ```

   Cette commande exécute l'image en tant que conteneur et crée un point de terminaison local à `localhost:9000/2015-03-31/functions/function/invocations`.

   > **Note**
   >
   > Si vous avez créé l'image Docker pour l'architecture du jeu d'instructions ARM64, veillez à utiliser l'option `--platform linux/arm64` plutôt que `--platform linux/amd64`.

2. À partir d'une nouvelle fenêtre de terminal, publiez un événement au point de terminaison local.

   Linux/macOS

   Sous Linux et macOS, exécutez la commande `curl` suivante :

   ```
   curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d '{}'
   ```

Cette commande invoque la fonction avec un événement vide et renvoie une réponse. Si vous utilisez votre propre code de fonction plutôt que l'exemple de code de fonction, vous pouvez invoquer la fonction avec une charge utile JSON. Exemple :

```
curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d
 '{"payload":"hello world!"}'
```

PowerShell

Dans PowerShell, exécutez la `Invoke-WebRequest` commande suivante :

```
Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/
invocations" -Method Post -Body '{}' -ContentType "application/json"
```

Cette commande invoque la fonction avec un événement vide et renvoie une réponse. Si vous utilisez votre propre code de fonction plutôt que l'exemple de code de fonction, vous pouvez invoquer la fonction avec une charge utile JSON. Exemple :

```
Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/
invocations" -Method Post -Body '{"payload":"hello world!"}' -ContentType
 "application/json"
```

3. Obtenez l'ID du conteneur.

```
docker ps
```

4. Utilisez la commande docker kill pour arrêter le conteneur. Dans cette commande, remplacez `3766c4ab331c` par l'ID du conteneur de l'étape précédente.

```
docker kill 3766c4ab331c
```

Déploiement de l'image

Pour charger l'image sur Amazon RIE et créer la fonction Lambda

1. Exécutez la commande get-login-password pour authentifier la CLI Docker auprès de votre registre Amazon ECR.

- Définissez la `--region` valeur à l' Région AWS endroit où vous souhaitez créer le référentiel Amazon ECR.
- `111122223333`Remplacez-le par votre Compte AWS identifiant.

```
aws ecr get-login-password --region us-east-1 | docker login --username AWS --
password-stdin 111122223333.dkr.ecr.us-east-1.amazonaws.com
```

2. Créez un référentiel dans Amazon ECR à l'aide de la commande create-repository.

```
aws ecr create-repository --repository-name hello-world --region us-east-1 --image-
scanning-configuration scanOnPush=true --image-tag-mutability MUTABLE
```

> **Note**
>
> Le référentiel Amazon ECR doit être Région AWS identique à la fonction Lambda.

En cas de succès, vous obtenez une réponse comme celle-ci :

```
{
    "repository": {
        "repositoryArn": "arn:aws:ecr:us-east-1:111122223333:repository/hello-
world",
        "registryId": "111122223333",
        "repositoryName": "hello-world",
        "repositoryUri": "111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-
world",
        "createdAt": "2023-03-09T10:39:01+00:00",
        "imageTagMutability": "MUTABLE",
        "imageScanningConfiguration": {
            "scanOnPush": true
        },
        "encryptionConfiguration": {
            "encryptionType": "AES256"
        }
    }
}
```

3. Copiez le `repositoryUri` à partir de la sortie de l'étape précédente.

4. Exécutez la commande docker tag pour étiqueter votre image locale dans votre référentiel Amazon ECR en tant que dernière version. Dans cette commande :

   - `docker-image:test` est le nom et la balise de votre image Docker. Il s'agit du nom et de la balise de l'image que vous avez spécifiés dans la commande `docker build`.
   - Remplacez `<ECRrepositoryUri>` par l'`repositoryUri` que vous avez copié. Assurez-vous d'inclure `:latest` à la fin de l'URI.

   ```
   docker tag docker-image:test <ECRrepositoryUri>:latest
   ```

   Exemple :

   ```
   docker tag docker-image:test 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
   ```

5. Exécutez la commande docker push pour déployer votre image locale dans le référentiel Amazon ECR. Assurez-vous d'inclure `:latest` à la fin de l'URI du référentiel.

   ```
   docker push 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
   ```

6. Créez un rôle d'exécution pour la fonction, si vous n'en avez pas déjà un. Vous aurez besoin de l'Amazon Resource Name (ARN) du rôle à l'étape suivante.
7. Créez la fonction Lambda. Pour `ImageUri`, indiquez l'URI du référentiel mentionné précédemment. Assurez-vous d'inclure `:latest` à la fin de l'URI.

   ```
   aws lambda create-function \
     --function-name hello-world \
     --package-type Image \
     --code ImageUri=111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \
     --role arn:aws:iam::111122223333:role/lambda-ex
   ```

   > **Note**
   >
   > Vous pouvez créer une fonction en utilisant une image d'un autre AWS compte, à condition que l'image se trouve dans la même région que la fonction Lambda. Pour plus d'informations, consultez Autorisations entre comptes Amazon ECR.

8. Invoquer la fonction.

```
aws lambda invoke --function-name hello-world response.json
```

Vous devriez obtenir une réponse comme celle-ci :

```
{
  "ExecutedVersion": "$LATEST",
  "StatusCode": 200
}
```

9. Pour voir la sortie de la fonction, consultez le fichier `response.json`.

Pour mettre à jour le code de la fonction, vous devez recréer l'image, charger la nouvelle image dans le référentiel Amazon ECR, puis utiliser la commande update-function-code pour déployer l'image dans la fonction Lambda.

Lambda résout l'étiquette d'image en hachage d'image spécifique. Cela signifie que si vous pointez la balise d'image qui a été utilisée pour déployer la fonction vers une nouvelle image dans Amazon ECR, Lambda ne met pas automatiquement à jour la fonction pour utiliser la nouvelle image.

Pour déployer la nouvelle image sur la même fonction Lambda, vous devez utiliser la commande update-function-code, même si la balise d'image dans Amazon ECR reste la même. Dans l'exemple suivant, l'option `--publish` crée une version de la fonction à l'aide de l'image du conteneur mise à jour.

```
aws lambda update-function-code \
  --function-name hello-world \
  --image-uri 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \
  --publish
```

Utilisation d'une autre image de base avec le client d'interface d'exécution

Si vous utilisez une image OS-only de base ou une image de base alternative, vous devez inclure le client d'interface d'exécution dans votre image. Le client d'interface d'exécution étend leAPI de runtime, qui gère l'interaction entre Lambda et votre code de fonction.

Installez le client d'interface d'exécution pour Python à l'aide du gestionnaire de packages pip :

```
pip install awslambdaric
```

Vous pouvez également télécharger le client d'interface d'exécution Python depuis GitHub.

L'exemple suivant montre comment créer une image de conteneur pour Python à l'aide d'une image non AWS basique. L'exemple Dockerfile utilise une image de base Python officielle. Le Dockerfile inclut le client d'interface d'exécution pour Python.

Conditions préalables

Pour exécuter la procédure indiquée dans cette section, vous devez satisfaire aux exigences suivantes :

- AWS CLI version 2
- Docker (version minimale 25.0.0)
- Le plug-in buildx Docker.
- Python

Création d'une image à partir d'une image de base alternative

Pour créer une image de conteneur à partir d'un objet autre que AWS image de base

1. Créez un répertoire pour le projet, puis passez à ce répertoire.

   ```
   mkdir example
   cd example
   ```

2. Créez un nouveau fichier appelé `lambda_function.py`. Vous pouvez ajouter l'exemple de code de fonction suivant au fichier pour le tester, ou utiliser le vôtre.

   Example Fonction Python

   ```
   import sys
   def handler(event, context):
       return 'Hello from AWS Lambda using Python' + sys.version + '!'
   ```

3. Créez un nouveau fichier appelé `requirements.txt`. Si vous utilisez l'exemple de code de fonction de l'étape précédente, vous pouvez laisser le fichier vide, car il n'y a pas de dépendances. Sinon, répertoriez chaque bibliothèque requise. Par exemple, voici à quoi votre fichier `requirements.txt` doit ressembler si votre fonction utilise AWS SDK pour Python (Boto3) :

Example requirements.txt

```
boto3
```

4. Créez un nouveau fichier Docker. Le Dockerfile suivant utilise une image de base Python officielle au lieu d'une image de base AWS. Le Dockerfile inclut le client d'interface d'exécution, ce qui rend l'image compatible avec Lambda. L'exemple de fichier Docker suivant utilise une génération en plusieurs étapes.

   - Définissez la propriété `FROM` sur l'image de base.
   - Définissez le `ENTRYPOINT` sur le module que vous souhaitez que le conteneur Docker exécute lorsqu'il démarre. Dans ce cas, le module est le client d'interface d'exécution.
   - Définissez le `CMD` sur le gestionnaire de la fonction Lambda.

   Notez que l'exemple de Dockerfile n'inclut pas d'instruction USER. Lorsque vous déployez une image de conteneur sur Lambda, Lambda définit automatiquement un utilisateur Linux par défaut disposant d'autorisations de moindre privilège. Ceci est différent du comportement standard de Docker qui est défini par défaut par l'utilisateur `root` lorsqu'aucune instruction `USER` n'est fournie.

   Example Dockerfile

```
# Define custom function directory
ARG FUNCTION_DIR="/function"

FROM python:3.12 AS build-image

# Include global arg in this stage of the build
ARG FUNCTION_DIR

# Copy function code
RUN mkdir -p ${FUNCTION_DIR}
COPY . ${FUNCTION_DIR}

# Install the function's dependencies
RUN pip install \
    --target ${FUNCTION_DIR} \
        awslambdaric
```

```
# Use a slim version of the base Python image to reduce the final image size
FROM python:3.12-slim

# Include global arg in this stage of the build
ARG FUNCTION_DIR
# Set working directory to function root directory
WORKDIR ${FUNCTION_DIR}

# Copy in the built dependencies
COPY --from=build-image ${FUNCTION_DIR} ${FUNCTION_DIR}

# Set runtime interface client as default command for the container runtime
ENTRYPOINT [ "/usr/local/bin/python", "-m", "awslambdaric" ]
# Pass the name of the function handler as an argument to the runtime
CMD [ "lambda_function.handler" ]
```

5. Générez l'image Docker à l'aide de la commande docker build. L'exemple suivant nomme l'image `docker-image` et lui donne la balise `test`. Pour rendre votre image compatible avec Lambda, vous devez utiliser l'option `--provenance=false`.

```
docker buildx build --platform linux/amd64 --provenance=false -t docker-image:test
 .
```

> **Note**
>
> La commande spécifie l'option `--platform linux/amd64` pour garantir la compatibilité de votre conteneur avec l'environnement d'exécution Lambda, quelle que soit l'architecture de votre machine de génération. Si vous avez l'intention de créer une fonction Lambda à l'aide de l'architecture du jeu d'instructions ARM64, veillez à modifier la commande pour utiliser plutôt l'option `--platform linux/arm64`.

(Facultatif) Testez l'image localement

Utilisez l'émulateur d'interface d'exécution pour tester l'image localement. Vous pouvez intégrer l'émulateur dans votre image ou utiliser la procédure suivante pour l'installer sur votre machine locale.

Pour installer et exécuter l'émulateur d'interface d'exécution sur votre ordinateur local

1. Depuis le répertoire de votre projet, exécutez la commande suivante pour télécharger l'émulateur d'interface d'exécution (architecture x86-64) GitHub et l'installer sur votre machine locale.

   Linux/macOS

   ```
   mkdir -p ~/.aws-lambda-rie && \
       curl -Lo ~/.aws-lambda-rie/aws-lambda-rie https://github.com/aws/aws-lambda-runtime-interface-emulator/releases/latest/download/aws-lambda-rie && \
       chmod +x ~/.aws-lambda-rie/aws-lambda-rie
   ```

   Pour installer l'émulateur arm64, remplacez l'URL du GitHub référentiel dans la commande précédente par la suivante :

   ```
   https://github.com/aws/aws-lambda-runtime-interface-emulator/releases/latest/download/aws-lambda-rie-arm64
   ```

   PowerShell

   ```
   $dirPath = "$HOME\.aws-lambda-rie"
   if (-not (Test-Path $dirPath)) {
       New-Item -Path $dirPath -ItemType Directory
   }

   $downloadLink = "https://github.com/aws/aws-lambda-runtime-interface-emulator/releases/latest/download/aws-lambda-rie"
   $destinationPath = "$HOME\.aws-lambda-rie\aws-lambda-rie"
   Invoke-WebRequest -Uri $downloadLink -OutFile $destinationPath
   ```

   Pour installer l'émulateur arm64, remplacez `$downloadLink` par ce qui suit :

   ```
   https://github.com/aws/aws-lambda-runtime-interface-emulator/releases/latest/download/aws-lambda-rie-arm64
   ```

2. Démarrez votre image Docker à l'aide de la commande docker run. Notez ce qui suit :

   - `docker-image` est le nom de l'image et `test` est la balise.
   - `/usr/local/bin/python -m awslambdaric lambda_function.handler` est le `ENTRYPOINT` suivi du `CMD` depuis votre Dockerfile.

Linux/macOS

```
docker run --platform linux/amd64 -d -v ~/.aws-lambda-rie:/aws-lambda -p
 9000:8080 \
    --entrypoint /aws-lambda/aws-lambda-rie \
    docker-image:test \
        /usr/local/bin/python -m awslambdaric lambda_function.handler
```

PowerShell

```
docker run --platform linux/amd64 -d -v "$HOME\.aws-lambda-rie:/aws-lambda" -p
 9000:8080 `
--entrypoint /aws-lambda/aws-lambda-rie `
docker-image:test `
    /usr/local/bin/python -m awslambdaric lambda_function.handler
```

Cette commande exécute l'image en tant que conteneur et crée un point de terminaison local à `localhost:9000/2015-03-31/functions/function/invocations`.

> **Note**
>
> Si vous avez créé l'image Docker pour l'architecture du jeu d'instructions ARM64, veillez à utiliser l'option `--platform linux/arm64` plutôt que `--platform linux/amd64`.

3. Publiez un événement au point de terminaison local.

Linux/macOS

Sous Linux et macOS, exécutez la commande `curl` suivante :

```
curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d '{}'
```

Cette commande invoque la fonction avec un événement vide et renvoie une réponse. Si vous utilisez votre propre code de fonction plutôt que l'exemple de code de fonction, vous pouvez invoquer la fonction avec une charge utile JSON. Exemple :

```
curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d
 '{"payload":"hello world!"}'
```

PowerShell

Dans PowerShell, exécutez la `Invoke-WebRequest` commande suivante :

```
Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/
invocations" -Method Post -Body '{}' -ContentType "application/json"
```

Cette commande invoque la fonction avec un événement vide et renvoie une réponse. Si vous utilisez votre propre code de fonction plutôt que l'exemple de code de fonction, vous pouvez invoquer la fonction avec une charge utile JSON. Exemple :

```
Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/
invocations" -Method Post -Body '{"payload":"hello world!"}' -ContentType
 "application/json"
```

4. Obtenez l'ID du conteneur.

```
docker ps
```

5. Utilisez la commande docker kill pour arrêter le conteneur. Dans cette commande, remplacez `3766c4ab331c` par l'ID du conteneur de l'étape précédente.

```
docker kill 3766c4ab331c
```

Déploiement de l'image

Pour charger l'image sur Amazon RIE et créer la fonction Lambda

1. Exécutez la commande get-login-password pour authentifier la CLI Docker auprès de votre registre Amazon ECR.
   - Définissez la `--region` valeur à l' Région AWS endroit où vous souhaitez créer le référentiel Amazon ECR.
   - `111122223333`Remplacez-le par votre Compte AWS identifiant.

```
aws ecr get-login-password --region us-east-1 | docker login --username AWS --
password-stdin 111122223333.dkr.ecr.us-east-1.amazonaws.com
```

2. Créez un référentiel dans Amazon ECR à l'aide de la commande create-repository.

```
aws ecr create-repository --repository-name hello-world --region us-east-1 --image-
scanning-configuration scanOnPush=true --image-tag-mutability MUTABLE
```

> **Note**
>
> Le référentiel Amazon ECR doit être Région AWS identique à la fonction Lambda.

En cas de succès, vous obtenez une réponse comme celle-ci :

```
{
    "repository": {
        "repositoryArn": "arn:aws:ecr:us-east-1:111122223333:repository/hello-
world",
        "registryId": "111122223333",
        "repositoryName": "hello-world",
        "repositoryUri": "111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-
world",
        "createdAt": "2023-03-09T10:39:01+00:00",
        "imageTagMutability": "MUTABLE",
        "imageScanningConfiguration": {
            "scanOnPush": true
        },
        "encryptionConfiguration": {
            "encryptionType": "AES256"
        }
    }
}
```

3. Copiez le `repositoryUri` à partir de la sortie de l'étape précédente.
4. Exécutez la commande docker tag pour étiqueter votre image locale dans votre référentiel Amazon ECR en tant que dernière version. Dans cette commande :

- `docker-image:test` est le nom et la balise de votre image Docker. Il s'agit du nom et de la balise de l'image que vous avez spécifiés dans la commande `docker build`.
- Remplacez `<ECRrepositoryUri>` par l'`repositoryUri` que vous avez copié. Assurez-vous d'inclure `:latest` à la fin de l'URI.

```
docker tag docker-image:test <ECRrepositoryUri>:latest
```

Exemple :

```
docker tag docker-image:test 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

5. Exécutez la commande docker push pour déployer votre image locale dans le référentiel Amazon ECR. Assurez-vous d'inclure `:latest` à la fin de l'URI du référentiel.

```
docker push 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

6. Créez un rôle d'exécution pour la fonction, si vous n'en avez pas déjà un. Vous aurez besoin de l'Amazon Resource Name (ARN) du rôle à l'étape suivante.
7. Créez la fonction Lambda. Pour `ImageUri`, indiquez l'URI du référentiel mentionné précédemment. Assurez-vous d'inclure `:latest` à la fin de l'URI.

```
aws lambda create-function \
  --function-name hello-world \
  --package-type Image \
  --code ImageUri=111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \
  --role arn:aws:iam::111122223333:role/lambda-ex
```

> **Note**
>
> Vous pouvez créer une fonction en utilisant une image d'un autre AWS compte, à condition que l'image se trouve dans la même région que la fonction Lambda. Pour plus d'informations, consultez Autorisations entre comptes Amazon ECR.

8. Invoquer la fonction.

```
aws lambda invoke --function-name hello-world response.json
```

Vous devriez obtenir une réponse comme celle-ci :

```
{
  "ExecutedVersion": "$LATEST",
  "StatusCode": 200
}
```

9. Pour voir la sortie de la fonction, consultez le fichier `response.json`.

Pour mettre à jour le code de la fonction, vous devez recréer l'image, charger la nouvelle image dans le référentiel Amazon ECR, puis utiliser la commande update-function-code pour déployer l'image dans la fonction Lambda.

Lambda résout l'étiquette d'image en hachage d'image spécifique. Cela signifie que si vous pointez la balise d'image qui a été utilisée pour déployer la fonction vers une nouvelle image dans Amazon ECR, Lambda ne met pas automatiquement à jour la fonction pour utiliser la nouvelle image.

Pour déployer la nouvelle image sur la même fonction Lambda, vous devez utiliser la commande update-function-code, même si la balise d'image dans Amazon ECR reste la même. Dans l'exemple suivant, l'option `--publish` crée une version de la fonction à l'aide de l'image du conteneur mise à jour.

```
aws lambda update-function-code \
  --function-name hello-world \
  --image-uri 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \
  --publish
```

Pour un exemple de création d'une image Python à partir d'une image de base Alpine, consultez Prise en charge des images conteneurs pour Lambda sur le blog AWS .

Utilisation de couches pour les fonctions d'événement Lambda en Python

Utilisez les couches Lambda pour empaqueter le code et les dépendances que vous souhaitez réutiliser dans plusieurs fonctions. Les couches contiennent généralement des dépendances de bibliothèque, une exécution personnalisée, ou des fichiers de configuration. La création d'une couche implique trois étapes générales :

1. Empaquetez le contenu de votre couche. Cela signifie créer une archive de fichiers .zip contenant les dépendances que vous souhaitez utiliser dans vos fonctions.
2. Créez la couche dans Lambda.
3. Ajoutez la couche à vos fonctions.

Rubriques

- Empaqueter le contenu de votre couche
- Créer la couche dans Lambda
- Ajouter la couche à votre fonction
- Exemple d'application

Empaqueter le contenu de votre couche

Pour créer une couche, regroupez vos packages dans une archive (fichier .zip) répondant aux exigences suivantes :

- Construisez la couche en utilisant la même version de Python que celle que vous prévoyez d'utiliser pour la fonction. Par exemple, si vous créez votre couche à l'aide de Python 3.14, utilisez le runtime Python 3.14 pour votre fonction.
- Votre fichier .zip doit inclure un répertoire `python` au niveau racine.
- Les packages de votre couche doivent être compatibles avec Linux. Les fonctions Lambda s'exécutent sur Amazon Linux.

Vous pouvez créer des couches contenant des bibliothèques Python tierces installées avec `pip` (comme `requests` ou `pandas`) ou vos propres modules et packages Python.

Third-party dépendances

Créer une couche à l'aide de packages pip

1. Choisissez l'une des méthodes suivantes pour installer les packages `pip` dans le répertoire de niveau supérieur requis (`python/`) :

   pip install

   Pour les packages Python purs (comme requests ou boto3) :

   ```
   pip install requests -t python/
   ```

   Certains packages Python, tels que NumPy Pandas, incluent des composants C compilés. Si vous créez une couche avec ces packages sous macOS ou Windows, vous devrez peut-être utiliser cette commande pour installer une Linux-compatible roue :

   ```
   pip install numpy --platform manylinux2014_x86_64 --only-binary=:all: -t python/
   ```

   Pour plus d'informations sur l'utilisation des packages Python contenant des composants compilés, consultez Création de packages de déploiement .zip avec des bibliothèques natives.

   requirements.txt

   L'utilisation d'un fichier `requirements.txt` vous permet de gérer les versions des packages et de garantir des installations cohérentes.

   Example requirements.txt

   ```
   requests==2.31.0
   boto3==1.37.34
   numpy==1.26.4
   ```

   Si votre fichier `requirements.txt` contient uniquement des packages Python purs (comme requests ou boto3) :

   ```
   pip install -r requirements.txt -t python/
   ```

Certains packages Python, tels que NumPy Pandas, incluent des composants C compilés. Si vous créez une couche avec ces packages sous macOS ou Windows, vous devrez peut-être utiliser cette commande pour installer une Linux-compatible roue :

```
pip install -r requirements.txt --platform manylinux2014_x86_64 --only-
binary=:all: -t python/
```

Pour plus d'informations sur l'utilisation des packages Python contenant des composants compilés, consultez Création de packages de déploiement .zip avec des bibliothèques natives.

2. Compressez le contenu du répertoire `python` dans un fichier .zip.

Linux/macOS

```
zip -r layer.zip python/
```

PowerShell

```
Compress-Archive -Path .\python -DestinationPath .\layer.zip
```

La structure de répertoire de votre fichier .zip devrait se présenter comme suit :

```
python/              # Required top-level directory
### requests/
### boto3/
### numpy/
### (dependencies of the other packages)
```

> **Note**
>
> Si vous utilisez un environnement virtuel Python (venv) pour installer des packages, la structure de votre répertoire est différente (par exemple,`python/lib/python3.x/site-packages`). Tant que votre fichier .zip inclut le répertoire `python` au niveau racine, Lambda peut localiser et importer vos packages.

Modules Python personnalisés

Créer une couche à l'aide de votre propre code

1. Créez le répertoire de niveau supérieur requis pour votre couche :

   ```
   mkdir python
   ```

2. Créez vos modules Python dans le répertoire `python`. L'exemple de module suivant valide les commandes en confirmant qu'elles contiennent les informations requises.

   Example module personnalisé : validator.py

   ```
   import json

   def validate_order(order_data):
       """Validates an order and returns formatted data."""
       required_fields = ['product_id', 'quantity']

       # Check required fields
       missing_fields = [field for field in required_fields if field not in
    order_data]
       if missing_fields:
           raise ValueError(f"Missing required fields: {', '.join(missing_fields)}")

       # Validate quantity
       quantity = order_data['quantity']
       if not isinstance(quantity, int) or quantity < 1:
           raise ValueError("Quantity must be a positive integer")

       # Format and return the validated data
       return {
           'product_id': str(order_data['product_id']),
           'quantity': quantity,
           'shipping_priority': order_data.get('priority', 'standard')
       }

   def format_response(status_code, body):
       """Formats the API response."""
       return {
           'statusCode': status_code,
           'body': json.dumps(body)
   ```

```
    }
```

3. Compressez le contenu du répertoire `python` dans un fichier .zip.

   Linux/macOS

   ```
   zip -r layer.zip python/
   ```

   PowerShell

   ```
   Compress-Archive -Path .\python -DestinationPath .\layer.zip
   ```

   La structure de répertoire de votre fichier .zip devrait se présenter comme suit :

   ```
   python/     # Required top-level directory
   ### validator.py
   ```

4. Dans votre fonction, importez et utilisez les modules comme vous le feriez avec n'importe quel package Python. Exemple :

   ```
   from validator import validate_order, format_response
   import json

   def lambda_handler(event, context):
       try:
           # Parse the order data from the event body
           order_data = json.loads(event.get('body', '{}'))

           # Validate and format the order
           validated_order = validate_order(order_data)

           return format_response(200, {
               'message': 'Order validated successfully',
               'order': validated_order
           })
       except ValueError as e:
           return format_response(400, {
               'error': str(e)
           })
       except Exception as e:
           return format_response(500, {
   ```

```
            'error': 'Internal server error'
        })
```

Vous pouvez utiliser l'événement de test suivant afin d'invoquer la fonction :

```
{
    "body": "{\"product_id\": \"ABC123\", \"quantity\": 2, \"priority\": \"express
\"}"
}
```

Réponse attendue :

```
{
  "statusCode": 200,
  "body": "{\"message\": \"Order validated successfully\", \"order\": {\"product_id
\": \"ABC123\", \"quantity\": 2, \"shipping_priority\": \"express\"}}"
}
```

Créer la couche dans Lambda

Vous pouvez publier votre couche à l'aide de la console Lambda AWS CLI ou de la console Lambda.

AWS CLI

Exécutez la AWS CLI commande publish-layer-version pour créer la couche Lambda :

```
aws lambda publish-layer-version --layer-name my-layer --zip-file fileb://layer.zip
 --compatible-runtimes python3.14
```

Le paramètre compatible runtimes est facultatif. Lorsqu'il est spécifié, Lambda utilise ce paramètre pour filtrer les couches dans la console Lambda.

Console

Pour créer une couche (console)

1. Ouvrez la page Couches de la console Lambda.
2. Sélectionnez Créer un calque.
3. Choisissez Charger un fichier .zip, puis chargez l'archive .zip que vous avez créée précédemment.

4. (Facultatif) Pour Exécutions compatibles, choisissez l'environnement d'exécution Python qui correspond à la version de Python que vous avez utilisée pour créer votre couche.
5. Cliquez sur Créer.

Ajouter la couche à votre fonction

AWS CLI

Pour associer la couche à votre fonction, exécutez la commande update-function-configuration AWS CLI . Utilisez l'ARN de la couche pour le paramètre `--layers`. L'ARN doit spécifier la version (par exemple, `arn:aws:lambda:us-east-1:123456789012:layer:my-layer:1`). Pour plus d'informations, consultez Couches et versions de couches.

```
aws lambda update-function-configuration --function-name my-function --cli-binary-format raw-in-base64-out --layers "arn:aws:lambda:us-east-1:123456789012:layer:my-layer:1"
```

L'cli-binary-formatoption est obligatoire si vous utilisez AWS CLI la version 2. Pour faire de ce paramètre le paramètre par défaut, exécutez `aws configure set cli-binary-format raw-in-base64-out`. Pour plus d'informations, consultez les options de ligne de commande globales AWS CLI prises en charge dans le Guide de l'utilisateur AWS Command Line Interface version 2.

Console

Ajouter une couche à une fonction

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez la fonction.
3. Faites défiler jusqu'à la section Couches, puis choisissez Ajouter une couche.
4. Sous Choisir une couche, sélectionnez Couches personnalisées, puis choisissez votre couche.

> **Note**
>
> Si vous n'avez pas ajouté d'environnement d'exécution compatible lors de la création de la couche, celle-ci ne sera pas répertoriée ici. Vous pouvez spécifier l'ARN de la couche à la place.

5. Choisissez Ajouter.

Exemple d’application

Pour d'autres exemples d'utilisation des couches Lambda, consultez l'exemple d'application layer-python dans le référentiel du AWS Lambda Developer Guide. GitHub Cette application inclut deux couches contenant des bibliothèques Python. Après avoir créé les couches, vous pouvez déployer et invoquer les fonctions correspondantes pour vérifier que les couches fonctionnent comme prévu.

Utilisation de l'objet de contexte Lambda pour récupérer les informations de la fonction d'événement Python

Lorsque Lambda exécute votre fonction d'événement, elle transmet un objet de contexte au gestionnaire. Cet objet fournit des méthodes et des propriétés fournissant des informations sur l'appel, la fonction et l'environnement d'exécution. Pour en savoir plus sur la façon dont l'objet de contexte est transmis au gestionnaire de fonctions, consultez Définir le gestionnaire de fonctions d'événement Lambda en Python.

Méthodes de contexte

- `get_remaining_time_in_millis` – Renvoie le nombre de millisecondes restant avant l'expiration de l'exécution.

Propriétés du contexte

- `function_name` – Nom de la fonction Lambda.
- `function_version` – Version de la fonction.
- `invoked_function_arn` – Amazon Resource Name (ARN) utilisé pour appeler la fonction. Indique si l'appelant a spécifié un numéro de version ou un alias.
- `memory_limit_in_mb` – Quantité de mémoire allouée à la fonction.
- `aws_request_id` – Identifiant de la demande d'invocation.
- `log_group_name` – Groupe de journaux pour la fonction.
- `log_stream_name` – Flux de journal de l'instance de fonction.
- `identity` – (applications mobiles) Informations sur l'identité Amazon Cognito qui a autorisé la demande.
  - `cognito_identity_id` – Identité Amazon Cognito authentifiée.
  - `cognito_identity_pool_id` – Groupe d'identités Amazon Cognito ayant autorisé l'invocation.
- `client_context` – (applications mobiles) Contexte client fourni à Lambda par l'application client.
  - `client.installation_id`
  - `client.app_title`
  - `client.app_version_name`
  - `client.app_version_code`

- `client.app_package_name`
- `custom` – `dict` de valeurs personnalisées définies par l'application client mobile.
- `env`— A `dict` des informations relatives à l'environnement fournies par le AWS SDK.

Powertools pour Lambda (Python) fournit une définition d'interface pour l'objet de contexte Lambda. Vous pouvez utiliser la définition de l'interface pour les indications de type ou pour examiner plus en détail la structure de l'objet de contexte Lambda. Pour la définition de l'interface, consultez le fichier lambda_context.py dans le référentiel powertools-lambda-python sur. GitHub

L'exemple suivant montre une fonction de gestionnaire qui consigne les informations de contexte.

Example handler.py

```
import time

def lambda_handler(event, context):
    print("Lambda function ARN:", context.invoked_function_arn)
    print("CloudWatch log stream name:", context.log_stream_name)
    print("CloudWatch log group name:",  context.log_group_name)
    print("Lambda Request ID:", context.aws_request_id)
    print("Lambda function memory limits in MB:", context.memory_limit_in_mb)
    # We have added a 1 second delay so you can see the time remaining in
 get_remaining_time_in_millis.
    time.sleep(1)
    print("Lambda time remaining in MS:", context.get_remaining_time_in_millis())
```

Outre les options répertoriées ci-dessus, vous pouvez également utiliser le AWS X-Ray SDK pour identifier les chemins Instrumentation du code Python dans AWS Lambda de code critiques, suivre leurs performances et capturer les données à des fins d'analyse.

Enregistrez et surveillez les fonctions d'événements Lambda en Python

AWS Lambda surveille automatiquement les fonctions Lambda et envoie des entrées de journal à Amazon. CloudWatch Votre fonction Lambda est fournie avec un groupe de CloudWatch journaux Logs et un flux de journaux pour chaque instance de votre fonction. L'environnement d'exécution Lambda envoie des détails sur chaque invocation et d'autres sorties provenant du code de votre fonction au flux de journaux. Pour plus d'informations sur CloudWatch les journaux, consultezEnvoi des journaux des fonctions d'événements Lambda aux journaux CloudWatch.

Pour produire des journaux à partir de votre code de fonction, vous pouvez utiliser le module intégré `logging`. Pour des entrées plus détaillées, vous pouvez utiliser n'importe quelle bibliothèque de journalisation qui écrit dans `stdout` ou `stderr`.

Impression dans le journal

Pour envoyer une sortie de base aux journaux, vous pouvez utiliser une méthode `print` dans votre fonction. L'exemple suivant enregistre les valeurs du groupe et du flux de CloudWatch journaux Logs, ainsi que l'objet d'événement.

Notez que si votre fonction génère des journaux à l'aide d'`print`instructions Python, Lambda ne peut envoyer les résultats de journal à CloudWatch Logs qu'au format texte brut. Pour capturer des journaux au format JSON structuré, vous devez utiliser une bibliothèque de journalisation prise en charge. Pour plus d'informations, consultez the section called "Utilisation des contrôles de journalisation avancés de Lambda avec Python".

Example lambda_function.py

```
import os
def lambda_handler(event, context):
    print('## ENVIRONMENT VARIABLES')
    print(os.environ['AWS_LAMBDA_LOG_GROUP_NAME'])
    print(os.environ['AWS_LAMBDA_LOG_STREAM_NAME'])
    print('## EVENT')
    print(event)
```

Example sortie de journal

```
START RequestId: 8f507cfc-xmpl-4697-b07a-ac58fc914c95 Version: $LATEST
## ENVIRONMENT VARIABLES
/aws/lambda/my-function
```

```
2025/08/31/[$LATEST]3893xmpl7fac4485b47bb75b671a283c
## EVENT
{'key': 'value'}
END RequestId: 8f507cfc-xmpl-4697-b07a-ac58fc914c95
REPORT RequestId: 8f507cfc-xmpl-4697-b07a-ac58fc914c95  Duration: 15.74 ms  Billed
 Duration: 147 ms Memory Size: 128 MB Max Memory Used: 56 MB  Init Duration: 130.49 ms
XRAY TraceId: 1-5e34a614-10bdxmplf1fb44f07bc535a1   SegmentId: 07f5xmpl2d1f6f85
 Sampled: true
```

L'environnement d'exécution Python enregistre les lignes `START`, `END` et `REPORT` pour chaque invocation. La ligne `REPORT` comprend les données suivantes :

Champs de données de la ligne REPORT

- RequestId— L'identifiant de demande unique pour l'invocation.
- Duration – Temps que la méthode de gestion du gestionnaire de votre fonction a consacré au traitement de l'événement.
- Billed Duration : temps facturé pour l'invocation.
- Memory Size – Quantité de mémoire allouée à la fonction.
- Max Memory Used – Quantité de mémoire utilisée par la fonction. Lorsque les appels partagent un environnement d'exécution, Lambda indique la mémoire maximale utilisée pour toutes les invocations. Ce comportement peut entraîner une valeur signalée plus élevée que prévu.
- Init Duration : pour la première requête servie, temps qu'il a pris à l'exécution charger la fonction et exécuter le code en dehors de la méthode du gestionnaire.
- XRAY TraceId — Pour les demandes suivies, l'ID de AWS X-Ray trace.
- SegmentId— Pour les demandes suivies, l'ID X-Ray du segment.
- Sampled : pour les demandes suivies, résultat de l'échantillonnage.

Utilisation d'une bibliothèque de journalisation

Pour des journaux plus détaillés, utilisez le module de journalisation de la bibliothèque standard, ou de toute bibliothèque de journalisation tierce qui écrit à `stdout` ou `stderr`.

Pour les environnements d'exécution Python pris en charge, vous pouvez choisir si les journaux créés à l'aide du module `logging` standard sont capturés en texte brut ou en JSON. Pour en savoir plus, consultez the section called "Utilisation des contrôles de journalisation avancés de Lambda avec Python".

Actuellement, le format de journal par défaut pour tous les environnements d'exécution Python est le texte brut. L'exemple suivant montre comment les sorties de journal créées à l'aide du `logging` module standard sont capturées en texte brut dans CloudWatch Logs.

```
import os
import logging
logger = logging.getLogger()
logger.setLevel("INFO")

def lambda_handler(event, context):
    logger.info('## ENVIRONMENT VARIABLES')
    logger.info(os.environ['AWS_LAMBDA_LOG_GROUP_NAME'])
    logger.info(os.environ['AWS_LAMBDA_LOG_STREAM_NAME'])
    logger.info('## EVENT')
    logger.info(event)
```

La sortie de `logger` inclut le niveau de journal, l'horodatage et l'ID de demande.

```
START RequestId: 1c8df7d3-xmpl-46da-9778-518e6eca8125 Version: $LATEST
[INFO]  2025-08-31T22:12:58.534Z    1c8df7d3-xmpl-46da-9778-518e6eca8125    ##
 ENVIRONMENT VARIABLES
[INFO]  2025-08-31T22:12:58.534Z    1c8df7d3-xmpl-46da-9778-518e6eca8125    /aws/
lambda/my-function
[INFO]  2025-08-31T22:12:58.534Z    1c8df7d3-xmpl-46da-9778-518e6eca8125    2025/01/31/
[$LATEST]1bbe51xmplb34a2788dbaa7433b0aa4d
[INFO]  2025-08-31T22:12:58.535Z    1c8df7d3-xmpl-46da-9778-518e6eca8125    ## EVENT
[INFO]  2025-08-31T22:12:58.535Z    1c8df7d3-xmpl-46da-9778-518e6eca8125    {'key':
 'value'}
END RequestId: 1c8df7d3-xmpl-46da-9778-518e6eca8125
REPORT RequestId: 1c8df7d3-xmpl-46da-9778-518e6eca8125  Duration: 2.75 ms   Billed
 Duration: 117 ms Memory Size: 128 MB Max Memory Used: 56 MB  Init Duration: 113.51 ms
XRAY TraceId: 1-5e34a66a-474xmpl7c2534a87870b4370   SegmentId: 073cxmpl3e442861
 Sampled: true
```

> **Note**
>
> Lorsque le format de journal de votre fonction est défini sur du texte brut, le paramètre de niveau de journal par défaut pour les environnements d'exécution Python est WARN. Cela signifie que Lambda envoie uniquement des sorties de journal de niveau WARN ou inférieur à CloudWatch Logs. Pour modifier le niveau de journalisation par défaut, utilisez la méthode

Python `logging` `setLevel()` comme indiqué dans cet exemple de code. Si vous définissez le format de journal de votre fonction sur JSON, nous vous recommandons de configurer le niveau de journalisation de votre fonction à l'aide de Lambda Advanced Logging Controls et non en définissant le niveau de journalisation dans le code. Pour en savoir plus, consultez the section called "Utilisation du filtrage au niveau du journal avec Python"

Utilisation des contrôles de journalisation avancés de Lambda avec Python

Pour mieux contrôler la manière dont les journaux de vos fonctions sont capturés, traités et consommés, vous pouvez configurer les options de journalisation suivantes pour les environnements d'exécution Lambda Python pris en charge :

- Format de journal : choisissez entre le format texte brut et le format JSON structuré pour les journaux de votre fonction
- Niveau de journalisation : pour les journaux au format JSON, choisissez le niveau de détail des journaux que Lambda envoie à Amazon CloudWatch, par exemple ERROR, DEBUG ou INFO
- Groupe de journaux : choisissez le groupe de CloudWatch journaux auquel votre fonction envoie les journaux

Pour plus d'informations sur ces options de journalisation et pour savoir comment configurer votre fonction pour les utiliser, consultez the section called "Configuration de contrôles de journalisation avancés pour les fonctions d'événement Lambda".

Pour en savoir plus sur l'utilisation du format de journal et des options de niveau de journal avec vos fonctions Python, consultez les instructions des sections suivantes.

Utilisation de journaux JSON structurés avec Python

Si vous sélectionnez JSON pour le format de journal de votre fonction, Lambda envoie les journaux produits par la bibliothèque de journalisation standard Python au CloudWatch format JSON structuré. Chaque objet de journal JSON contient au moins quatre paires clé-valeur avec les clés suivantes :

- `"timestamp"` - heure à laquelle le message de journal a été généré
- `"level"` - niveau de journalisation attribué au message
- `"message"` - contenu du message de journal
- `"requestId"` - identifiant unique de la demande pour l'invocation de la fonction

La bibliothèque Python `logging` peut également ajouter des paires clé-valeur supplémentaires, comme `"logger"`, dans cet objet JSON.

Les exemples présentés dans les sections suivantes montrent comment les sorties de journal générées à l'aide de la `logging` bibliothèque Python sont capturées dans CloudWatch Logs lorsque vous configurez le format de journal de votre fonction au format JSON.

Notez que si vous utilisez la `print` méthode pour produire des sorties de journal de base comme décrit dansthe section called “Impression dans le journal”, Lambda capture ces sorties sous forme de texte brut, même si vous configurez le format de journalisation de votre fonction au format JSON.

Sorties JSON standard à l’aide de la bibliothèque de journalisation Python

Les exemples d'extrait de code et de sortie de journal suivants montrent comment les sorties de journal standard générées à l'aide de la `logging` bibliothèque Python sont capturées dans CloudWatch Logs lorsque le format de journal de votre fonction est défini sur JSON.

Example Code de journalisation Python

```
import logging
logger = logging.getLogger()

def lambda_handler(event, context):
    logger.info("Inside the handler function")
```

Example Enregistrement de journaux JSON

```
{
    "timestamp":"2025-10-27T19:17:45.586Z",
    "level":"INFO",
    "message":"Inside the handler function",
    "logger": "root",
    "requestId":"79b4f56e-95b1-4643-9700-2807f4e68189"
}
```

Enregistrement de paramètres supplémentaires au format JSON

Lorsque le journal de votre fonction est au format JSON, vous pouvez également journaliser des paramètres supplémentaires avec la bibliothèque `logging` Python standard en utilisant le mot-clé `extra` pour transmettre un dictionnaire Python à la sortie du journal.

Example Code de journalisation Python

```
import logging

def lambda_handler(event, context):
    logging.info(
        "extra parameters example",
        extra={"a":"b", "b": [3]},
    )
```

Example Enregistrement de journaux JSON

```
{
  "timestamp": "2025-11-02T15:26:28Z",
  "level": "INFO",
  "message": "extra parameters example",
  "logger": "root",
  "requestId": "3dbd5759-65f6-45f8-8d7d-5bdc79a3bd01",
  "a": "b",
  "b": [
    3
  ]
}
```

Exceptions de journalisation au format JSON

L'extrait de code suivant montre comment les exceptions Python sont capturées dans la sortie du journal de votre fonction lorsque vous définissez le format de journal sur JSON. Notez que les sorties de journal générées en utilisant `logging.exception` sont affectées au niveau de journal ERROR.

Example Code de journalisation Python

```
import logging

def lambda_handler(event, context):
    try:
        raise Exception("exception")
    except:
        logging.exception("msg")
```

Example Enregistrement de journaux JSON

```
{
  "timestamp": "2025-11-02T16:18:57Z",
  "level": "ERROR",
  "message": "msg",
  "logger": "root",
  "stackTrace": [
    "  File \"/var/task/lambda_function.py\", line 15, in lambda_handler\n    raise
 Exception(\"exception\")\n"
  ],
  "errorType": "Exception",
  "errorMessage": "exception",
  "requestId": "3f9d155c-0f09-46b7-bdf1-e91dab220855",
  "location": "/var/task/lambda_function.py:lambda_handler:17"
}
```

Journaux structurés JSON avec d'autres outils de journalisation

Si votre code utilise déjà une autre bibliothèque de journalisation, telle que Powertools for AWS Lambda, pour produire des journaux structurés en JSON, vous n'avez pas besoin d'apporter de modifications. AWS Lambda ne double code aucun journal déjà codé au format JSON. Même si vous configurez votre fonction pour utiliser le format de journal JSON, vos sorties de journalisation apparaissent CloudWatch dans la structure JSON que vous définissez.

L'exemple suivant montre comment les sorties de journal générées à l'aide du AWS Lambda package Powertools for sont capturées dans CloudWatch Logs. Le format de cette sortie de journal est le même, que la configuration de journalisation de votre fonction soit définie sur JSON ou TEXT. Pour plus d'informations sur l'utilisation de Powertools pour AWS Lambda, consultez the section called “Utilisation de Powertools pour AWS Lambda (Python) et AWS SAM pour une journalisation structurée” et the section called “Utilisation de Powertools pour AWS Lambda (Python) et AWS CDK pour une journalisation structurée”

Example Extrait de code de journalisation en Python (à l'aide de Powertools pour AWS Lambda)

```
from aws_lambda_powertools import Logger

logger = Logger()

def lambda_handler(event, context):
    logger.info("Inside the handler function")
```

Example Enregistrement de journal JSON (à l'aide de Powertools pour AWS Lambda)

```
{
    "level": "INFO",
    "location": "lambda_handler:7",
    "message": "Inside the handler function",
    "timestamp": "2025-10-31 22:38:21,010+0000",
    "service": "service_undefined",
    "xray_trace_id": "1-654181dc-65c15d6b0fecbdd1531ecb30"
}
```

Utilisation du filtrage au niveau du journal avec Python

En configurant le filtrage au niveau des journaux, vous pouvez choisir de n'envoyer que les journaux d'un certain niveau de journalisation ou inférieur à CloudWatch Logs. Pour savoir comment configurer le filtrage de niveau journal de votre fonction, consultez the section called “Log-level filtrage”.

AWS Lambda Pour filtrer les journaux de votre application en fonction de leur niveau de journalisation, votre fonction doit utiliser des journaux au format JSON. Vous pouvez effectuer cette opération de deux façons :

- Créez des sorties de journal à l'aide de la `logging` bibliothèque Python standard et configurez votre fonction pour utiliser le format de journal JSON. AWS Lambda filtre ensuite les sorties de votre journal à l'aide de la paire clé-valeur « niveau » de l'objet JSON décrit dansthe section called “Utilisation de journaux JSON structurés avec Python”. Pour savoir comment configurer le format de journal de votre fonction, consultezthe section called “Configuration de contrôles de journalisation avancés pour les fonctions d'événement Lambda”.
- Utilisez une autre bibliothèque ou méthode de journalisation pour créer des journaux structurés JSON dans votre code qui incluent une paire clé-valeur « niveau » définissant le niveau de sortie du journal. Par exemple, vous pouvez utiliser Powertools pour générer des sorties AWS Lambda de journal structurées JSON à partir de votre code.

  Vous pouvez également utiliser une instruction print pour générer un objet JSON contenant un identifiant de niveau de journalisation. L'instruction d'impression suivante produit une sortie au format JSON dans laquelle le niveau de journalisation est défini sur INFO. AWS Lambda envoie l'objet JSON à CloudWatch Logs si le niveau de journalisation de votre fonction est défini sur INFO, DEBUG ou TRACE.

  ```
  print('{"msg":"My log message", "level":"info"}')
  ```

Pour que Lambda puisse filtrer les journaux de votre fonction, vous devez également inclure une paire `"timestamp"` clé-valeur dans la sortie de votre journal JSON. L'heure doit être spécifiée dans un format d'horodatage RFC 3339 valide. Si vous ne fournissez pas d'horodatage valide, Lambda attribue au journal le niveau INFO et ajoute un horodatage pour vous.

Affichage des journaux dans la console Lambda

Vous pouvez utiliser la console Lambda pour consulter les résultats du journal après avoir invoqué une fonction d'événement Lambda.

Si votre code peut être testé à partir de l'éditeur de code intégré, vous trouverez des journaux dans les résultats d'exécution. Lorsque vous utilisez la fonctionnalité de test de la console pour appeler une fonction, vous trouverez la sortie du journal dans la section Détails.

Afficher les journaux dans CloudWatch la console

Vous pouvez utiliser la CloudWatch console Amazon pour consulter les journaux de toutes les invocations de la fonction d'événement Lambda.

Pour afficher les journaux sur la CloudWatch console

1. Ouvrez la page Groupes de journaux sur la CloudWatch console.
2. Choisissez le groupe de journaux pour votre fonction (/aws/lambda/***your-function-name***).
3. Choisissez un flux de journaux.

Chaque flux de journal correspond à une instance de votre fonction. Un flux de journal apparaît lorsque vous mettez à jour votre fonction Lambda et lorsque des instances supplémentaires sont créées pour gérer les appels simultanés. Pour trouver les journaux d'un appel spécifique, nous vous recommandons d'instrumenter votre fonction avec. AWS X-Ray X-Ray enregistre les détails de la demande et du flux de log dans la trace.

Afficher les journaux avec AWS CLI

AWS CLI Il s'agit d'un outil open source que vous pouvez utiliser pour interagir avec les AWS services à l'aide de commandes dans votre interface de ligne de commande. Pour effectuer les étapes de cette section, vous devez disposer de la version 2 de l'AWS CLI.

Vous pouvez utiliser AWS CLI pour récupérer les journaux d'une invocation à l'aide de l'option de commande `--log-type`. La réponse inclut un champ `LogResult` qui contient jusqu'à 4 Ko de journaux codés en base64 provenant de l'invocation.

Example récupérer un ID de journal

L'exemple suivant montre comment récupérer un ID de journal à partir du champ `LogResult` d'une fonction nommée `my-function`.

```
aws lambda invoke --function-name my-function out --log-type Tail
```

Vous devriez voir la sortie suivante:

```
{
    "StatusCode": 200,
    "LogResult":
 "U1RBUlQgUmVxdWVzdElkOiA4N2QwNDRiOC1mMTU0LTExZTgtOGNkYS0yOTc0YzVlNGZiMjEgVmVyc2lvb...",
    "ExecutedVersion": "$LATEST"
}
```

Example décoder les journaux

Dans la même invite de commandes, utilisez l'utilitaire `base64` pour décoder les journaux. L'exemple suivant montre comment récupérer les journaux encodés en base64 pour `my-function`.

```
aws lambda invoke --function-name my-function out --log-type Tail \
--query 'LogResult' --output text --cli-binary-format raw-in-base64-out | base64 --
decode
```

L'cli-binary-formatoption est obligatoire si vous utilisez AWS CLI la version 2. Pour faire de ce paramètre le paramètre par défaut, exécutez `aws configure set cli-binary-format raw-in-base64-out`. Pour plus d'informations, consultez les options de ligne de commande globales AWS CLI prises en charge dans le Guide de l'utilisateur AWS Command Line Interface version 2.

Vous devriez voir la sortie suivante :

```
START RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8 Version: $LATEST
"AWS_SESSION_TOKEN": "AgoJb3JpZ2luX2VjELj...", "_X_AMZN_TRACE_ID": "Root=1-5d02e5ca-
f5792818b6fe8368e5b51d50;Parent=191db58857df8395;Sampled=0"",ask/lib:/opt/lib",
END RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8
REPORT RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8  Duration: 79.67 ms      Billed
 Duration: 80 ms         Memory Size: 128 MB     Max Memory Used: 73 MB
```

L'utilitaire `base64` est disponible sous Linux, macOS et Ubuntu sous Windows. Les utilisateurs de macOS auront peut-être besoin d'utiliser `base64 -D`.

Example Script get-logs.sh

Dans la même invite de commandes, utilisez le script suivant pour télécharger les cinq derniers événements de journalisation. Le script utilise `sed` pour supprimer les guillemets du fichier de sortie et attend 15 secondes pour permettre la mise à disposition des journaux. La sortie comprend la réponse de Lambda, ainsi que la sortie de la commande `get-log-events`.

Copiez le contenu de l'exemple de code suivant et enregistrez-le dans votre répertoire de projet Lambda sous `get-logs.sh`.

L'cli-binary-formatoption est obligatoire si vous utilisez AWS CLI la version 2. Pour faire de ce paramètre le paramètre par défaut, exécutez `aws configure set cli-binary-format raw-in-base64-out`. Pour plus d'informations, consultez les options de ligne de commande globales AWS CLI prises en charge dans le Guide de l'utilisateur AWS Command Line Interface version 2.

```
#!/bin/bash
aws lambda invoke --function-name my-function --cli-binary-format raw-in-base64-out --
payload '{"key": "value"}' out
sed -i'' -e 's/"//g' out
sleep 15
aws logs get-log-events --log-group-name /aws/lambda/my-function --log-stream-
name stream1 --limit 5
```

Example macOS et Linux (uniquement)

Dans la même invite de commande, les utilisateurs de macOS et de Linux devront peut-être exécuter la commande suivante pour s'assurer que le script est exécutable.

```
chmod -R 755 get-logs.sh
```

Example récupérer les cinq derniers événements de journal

Dans la même invite de commande, exécutez le script suivant pour obtenir les cinq derniers événements de journalisation.

```
./get-logs.sh
```

Vous devriez voir la sortie suivante:

```
{
    "StatusCode": 200,
```

```
    "ExecutedVersion": "$LATEST"
}
{
    "events": [
        {
            "timestamp": 1559763003171,
            "message": "START RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf Version:
 $LATEST\n",
            "ingestionTime": 1559763003309
        },
        {
            "timestamp": 1559763003173,
            "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tENVIRONMENT VARIABLES\r{\r  \"AWS_LAMBDA_FUNCTION_VERSION\": \"$LATEST\",
\r ...",
            "ingestionTime": 1559763018353
        },
        {
            "timestamp": 1559763003173,
            "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tEVENT\r{\r  \"key\": \"value\"\r}\n",
            "ingestionTime": 1559763018353
        },
        {
            "timestamp": 1559763003218,
            "message": "END RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf\n",
            "ingestionTime": 1559763018353
        },
        {
            "timestamp": 1559763003218,
            "message": "REPORT RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tDuration: 26.73 ms\tBilled Duration: 27 ms \tMemory Size: 128 MB\tMax Memory Used: 75
 MB\t\n",
            "ingestionTime": 1559763018353
        }
    ],
    "nextForwardToken": "f/34783877304859518393868359594929986069206639495374241795",
    "nextBackwardToken": "b/34783877303811383369537420289090800615709599058929582080"
}
```

Suppression de journaux

Les groupes de journaux ne sont pas supprimés automatiquement quand vous supprimez une fonction. Pour éviter de stocker des journaux indéfiniment, supprimez le groupe de journaux ou configurez une période de conservation à l'issue de laquelle les journaux sont supprimés automatiquement.

Utilisation d'autres outils et bibliothèques de journalisation

Powertools for AWS Lambda (Python) est une boîte à outils destinée aux développeurs qui permet de mettre en œuvre les meilleures pratiques sans serveur et d'accroître la rapidité des développeurs. L'utilitaire Logger fournit un enregistreur optimisé pour Lambda qui inclut des informations supplémentaires sur le contexte de fonction pour toutes vos fonctions avec une sortie structurée en JSON. Utilisez cet utilitaire pour effectuer les opérations suivantes :

- Capturer les champs clés du contexte Lambda, démarrer à froid et structurer la sortie de la journalisation sous forme de JSON
- Journaliser les événements d'invocation Lambda lorsque cela est demandé (désactivé par défaut)
- Imprimer tous les journaux uniquement pour un pourcentage d'invocations via l'échantillonnage des journaux (désactivé par défaut)
- Ajouter des clés supplémentaires au journal structuré à tout moment
- Utiliser un formateur de journaux personnalisé (Apportez votre propre formateur) pour produire des journaux dans une structure compatible avec le RFC de journalisation de votre organisation

Utilisation de Powertools pour AWS Lambda (Python) et AWS SAM pour une journalisation structurée

Suivez les étapes ci-dessous pour télécharger, créer et déployer un exemple d'application Hello World Python avec des modules Powertools for Python (français non garanti) intégrés à l'aide d'AWS SAM. Cette application met en œuvre un backend API de base et utilise Powertools pour émettre des journaux, des métriques et des traces. Il se compose d'un point de terminaison Amazon API Gateway et d'une fonction d'événement Lambda. Lorsque vous envoyez une requête GET au point de terminaison API Gateway, la fonction invoque, envoie des journaux et des métriques à l'aide du format métrique intégré à CloudWatch, et envoie des traces à AWS X-Ray. La fonction renvoie un message `hello world`.

Conditions préalables

Pour exécuter la procédure indiquée dans cette section, vous devez satisfaire aux exigences suivantes :

- Python 3.9
- AWS CLI version 2
- AWS SAM CLI version 1.75 ou ultérieure. Si vous disposez d'une ancienne version de la AWS SAM CLI, consultez la section Mise à niveau de la AWS SAM CLI.

Déployer un échantillon AWS SAM vigie

1. Initialisez l'application à l'aide du modèle Hello World Python.

```
sam init --app-template hello-world-powertools-python --name sam-app --package-type
 Zip --runtime python3.9 --no-tracing
```

2. Créez l'application.

```
cd sam-app && sam build
```

3. Déployez l'application.

```
sam deploy --guided
```

4. Suivez les invites à l'écran. Appuyez sur `Enter` pour accepter les options par défaut fournies dans l'expérience interactive.

> **Note**
>
> Car l'autorisation n'a HelloWorldFunction peut-être pas été définie, est-ce que ça va ? , assurez-vous de participery.

5. Obtenez l'URL de l'application déployée :

```
aws cloudformation describe-stacks --stack-name sam-app --query
 'Stacks[0].Outputs[?OutputKey==`HelloWorldApi`].OutputValue' --output text
```

6. Invoquez le point de terminaison de l'API :

```
curl GET <URL_FROM_PREVIOUS_STEP>
```

En cas de succès, vous obtiendrez cette réponse :

```
{"message":"hello world"}
```

7. Pour obtenir les journaux de la fonction, exécutez sam logs. Pour en savoir plus, consultez Utilisation des journaux dans le Guide du développeur AWS Serverless Application Model .

```
sam logs --stack-name sam-app
```

La sortie du journal se présente comme suit :

```
2025/02/03/[$LATEST]ea9a64ec87294bf6bbc9026c05a01e04
 2025-02-03T14:59:50.371000 INIT_START Runtime Version:
 python:3.9.v16    Runtime Version ARN: arn:aws:lambda:us-
east-1::runtime:07a48df201798d627f2b950f03bb227aab4a655a1d019c3296406f95937e2525
2025/02/03/[$LATEST]ea9a64ec87294bf6bbc9026c05a01e04 2025-02-03T14:59:51.112000
 START RequestId: d455cfc4-7704-46df-901b-2a5cce9405be Version: $LATEST
2025/02/03/[$LATEST]ea9a64ec87294bf6bbc9026c05a01e04 2025-02-03T14:59:51.114000 {
  "level": "INFO",
  "location": "hello:23",
  "message": "Hello world API - HTTP 200",
  "timestamp": "2025-02-03 14:59:51,113+0000",
  "service": "PowertoolsHelloWorld",
  "cold_start": true,
  "function_name": "sam-app-HelloWorldFunction-YBg8yfYtOc9j",
  "function_memory_size": "128",
  "function_arn": "arn:aws:lambda:us-east-1:111122223333:function:sam-app-
HelloWorldFunction-YBg8yfYtOc9j",
  "function_request_id": "d455cfc4-7704-46df-901b-2a5cce9405be",
  "correlation_id": "e73f8aef-5e07-436e-a30b-63e4b23f0047",
  "xray_trace_id": "1-63dd2166-434a12c22e1307ff2114f299"
}
2025/02/03/[$LATEST]ea9a64ec87294bf6bbc9026c05a01e04 2025-02-03T14:59:51.126000 {
  "_aws": {
    "Timestamp": 1675436391126,
    "CloudWatchMetrics": [
      {
        "Namespace": "Powertools",
        "Dimensions": [
```

```
          [
            "function_name",
            "service"
          ]
        ],
        "Metrics": [
          {
            "Name": "ColdStart",
            "Unit": "Count"
          }
        ]
      }
    ]
  },
  "function_name": "sam-app-HelloWorldFunction-YBg8yfYtOc9j",
  "service": "PowertoolsHelloWorld",
  "ColdStart": [
    1.0
  ]
}
2025/02/03/[$LATEST]ea9a64ec87294bf6bbc9026c05a01e04 2025-02-03T14:59:51.126000 {
  "_aws": {
    "Timestamp": 1675436391126,
    "CloudWatchMetrics": [
      {
        "Namespace": "Powertools",
        "Dimensions": [
          [
            "service"
          ]
        ],
        "Metrics": [
          {
            "Name": "HelloWorldInvocations",
            "Unit": "Count"
          }
        ]
      }
    ]
  },
  "service": "PowertoolsHelloWorld",
  "HelloWorldInvocations": [
    1.0
  ]
```

```
}
2025/02/03/[$LATEST]ea9a64ec87294bf6bbc9026c05a01e04 2025-02-03T14:59:51.128000 END
 RequestId: d455cfc4-7704-46df-901b-2a5cce9405be
2025/02/03/[$LATEST]ea9a64ec87294bf6bbc9026c05a01e04 2025-02-03T14:59:51.128000
 REPORT RequestId: d455cfc4-7704-46df-901b-2a5cce9405be    Duration: 16.33 ms
 Billed Duration: 756 ms    Memory Size: 128 MB    Max Memory Used: 64 MB    Init
 Duration: 739.46 ms
XRAY TraceId: 1-63dd2166-434a12c22e1307ff2114f299    SegmentId: 3c5d18d735a1ced0
 Sampled: true
```

8. Il s'agit d'un point de terminaison d'API public accessible par Internet. Nous vous recommandons de supprimer le point de terminaison après un test.

```
sam delete
```

Gestion de la conservation des journaux

Les groupes de journaux ne sont pas supprimés automatiquement quand vous supprimez une fonction. Pour éviter de stocker les journaux indéfiniment, supprimez le groupe de journaux ou configurez une période de conservation après laquelle les journaux CloudWatch sont automatiquement supprimés. Pour configurer la conservation des journaux, ajoutez ce qui suit à votre AWS SAM modèle :

```
Resources:
  HelloWorldFunction:
    Type: AWS::Serverless::Function
    Properties:
      # Omitting other properties

  LogGroup:
    Type: AWS::Logs::LogGroup
    Properties:
      LogGroupName: !Sub "/aws/lambda/${HelloWorldFunction}"
      RetentionInDays: 7
```

Utilisation de Powertools pour AWS Lambda (Python) et AWS CDK pour une journalisation structurée

Suivez les étapes ci-dessous pour télécharger, créer et déployer un exemple d'application Hello World Python avec des modules Powertools pour AWS Lambda (Python) intégrés à l'aide du AWS CDK. Cette application met en œuvre un backend API de base et utilise Powertools pour émettre

des journaux, des métriques et des traces. Il se compose d'un point de terminaison Amazon API Gateway et d'une fonction d'événement Lambda. Lorsque vous envoyez une requête GET au point de terminaison API Gateway, la fonction invoque, envoie des journaux et des métriques à l'aide du format métrique intégré à CloudWatch, et envoie des traces à AWS X-Ray. La fonction renvoie un message hello world.

Conditions préalables

Pour exécuter la procédure indiquée dans cette section, vous devez satisfaire aux exigences suivantes :

- Python 3.9
- AWS CLI version 2
- AWS CDK version 2
- AWS SAM CLI version 1.75 ou ultérieure. Si vous disposez d'une ancienne version de la AWS SAM CLI, consultez la section Mise à niveau de la AWS SAM CLI.

Déployer un échantillon AWS CDK vigie

1. Créez un répertoire de projets pour votre nouvelle application.

```
mkdir hello-world
cd hello-world
```

2. Initialisez l'application.

```
cdk init app --language python
```

3. Installez les dépendances de Python.

```
pip install -r requirements.txt
```

4. Créez un répertoire lambda_function dans le dossier racine.

```
mkdir lambda_function
cd lambda_function
```

5. Créez un fichier app.py et ajoutez-y le code suivant. Il s'agit du code de la fonction .

```
from aws_lambda_powertools.event_handler import APIGatewayRestResolver
```

```
from aws_lambda_powertools.utilities.typing import LambdaContext
from aws_lambda_powertools.logging import correlation_paths
from aws_lambda_powertools import Logger
from aws_lambda_powertools import Tracer
from aws_lambda_powertools import Metrics
from aws_lambda_powertools.metrics import MetricUnit

app = APIGatewayRestResolver()
tracer = Tracer()
logger = Logger()
metrics = Metrics(namespace="PowertoolsSample")

@app.get("/hello")
@tracer.capture_method
def hello():
    # adding custom metrics
    # See: https://docs.aws.amazon.com/powertools/python/latest//latest/core/
metrics/
    metrics.add_metric(name="HelloWorldInvocations", unit=MetricUnit.Count,
 value=1)

    # structured log
    # See: https://docs.aws.amazon.com/powertools/python/latest//latest/core/
logger/
    logger.info("Hello world API - HTTP 200")
    return {"message": "hello world"}

# Enrich logging with contextual information from Lambda
@logger.inject_lambda_context(correlation_id_path=correlation_paths.API_GATEWAY_REST)
# Adding tracer
# See: https://docs.aws.amazon.com/powertools/python/latest//latest/core/tracer/
@tracer.capture_lambda_handler
# ensures metrics are flushed upon request completion/failure and capturing
 ColdStart metric
@metrics.log_metrics(capture_cold_start_metric=True)
def lambda_handler(event: dict, context: LambdaContext) -> dict:
    return app.resolve(event, context)
```

6. Ouvrez le répertoire hello_world. Vous devriez voir un fichier nommé hello_world_stack.py.

```
cd ..
cd hello_world
```

7. Ouvrez hello_world_stack.py et ajoutez le code suivant au fichier. Il contient le constructeur Lambda, qui crée la fonction, configure les variables d'environnement pour Powertools et définit la durée de conservation des journaux à une semaine, et le constructeur ApiGatewayv 1, qui crée l'API REST.

```
from aws_cdk import (
    Stack,
    aws_apigateway as apigwv1,
    aws_lambda as lambda_,
    CfnOutput,
    Duration
)
from constructs import Construct

class HelloWorldStack(Stack):

    def __init__(self, scope: Construct, construct_id: str, **kwargs) -> None:
        super().__init__(scope, construct_id, **kwargs)

        # Powertools Lambda Layer
        powertools_layer = lambda_.LayerVersion.from_layer_version_arn(
            self,
            id="lambda-powertools",
            # Using AWS Lambda Powertools with Lambda Layer
            # This imports the Powertools layer which provides observability
 features for Lambda functions
            # For available versions, see: https://docs.aws.amazon.com/powertools/
python/latest/#lambda-layer
        )

        function = lambda_.Function(self,
            'sample-app-lambda',
            runtime=lambda_.Runtime.PYTHON_3_9,
            layers=[powertools_layer],
            code = lambda_.Code.from_asset("./lambda_function/"),
            handler="app.lambda_handler",
            memory_size=128,
            timeout=Duration.seconds(3),
            architecture=lambda_.Architecture.X86_64,
            environment={
                "POWERTOOLS_SERVICE_NAME": "PowertoolsHelloWorld",
                "POWERTOOLS_METRICS_NAMESPACE": "PowertoolsSample",
                "LOG_LEVEL": "INFO"
```

```
            }
        )

        apigw = apigwv1.RestApi(self, "PowertoolsAPI",
 deploy_options=apigwv1.StageOptions(stage_name="dev"))

        hello_api = apigw.root.add_resource("hello")
        hello_api.add_method("GET", apigwv1.LambdaIntegration(function,
 proxy=True))

        CfnOutput(self, "apiUrl", value=f"{apigw.url}hello")
```

8. Déployez votre application.

```
cd ..
cdk deploy
```

9. Obtenez l'URL de l'application déployée :

```
aws cloudformation describe-stacks --stack-name HelloWorldStack --query
 'Stacks[0].Outputs[?OutputKey==`apiUrl`].OutputValue' --output text
```

10. Invoquez le point de terminaison de l'API :

```
curl GET <URL_FROM_PREVIOUS_STEP>
```

    En cas de succès, vous obtiendrez cette réponse :

```
{"message":"hello world"}
```

11. Pour obtenir les journaux de la fonction, exécutez sam logs. Pour en savoir plus, consultez Utilisation des journaux dans le Guide du développeur AWS Serverless Application Model .

```
sam logs --stack-name HelloWorldStack
```

    La sortie du journal se présente comme suit :

```
2025/02/03/[$LATEST]ea9a64ec87294bf6bbc9026c05a01e04
 2025-02-03T14:59:50.371000 INIT_START Runtime Version:
 python:3.9.v16    Runtime Version ARN: arn:aws:lambda:us-
east-1::runtime:07a48df201798d627f2b950f03bb227aab4a655a1d019c3296406f95937e2525
```

```
2025/02/03/[$LATEST]ea9a64ec87294bf6bbc9026c05a01e04 2025-02-03T14:59:51.112000
 START RequestId: d455cfc4-7704-46df-901b-2a5cce9405be Version: $LATEST
2025/02/03/[$LATEST]ea9a64ec87294bf6bbc9026c05a01e04 2025-02-03T14:59:51.114000 {
  "level": "INFO",
  "location": "hello:23",
    "message": "Hello world API - HTTP 200",
  "timestamp": "2025-02-03 14:59:51,113+0000",
  "service": "PowertoolsHelloWorld",
  "cold_start": true,
  "function_name": "sam-app-HelloWorldFunction-YBg8yfYtOc9j",
  "function_memory_size": "128",
  "function_arn": "arn:aws:lambda:us-east-1:111122223333:function:sam-app-
HelloWorldFunction-YBg8yfYtOc9j",
  "function_request_id": "d455cfc4-7704-46df-901b-2a5cce9405be",
  "correlation_id": "e73f8aef-5e07-436e-a30b-63e4b23f0047",
  "xray_trace_id": "1-63dd2166-434a12c22e1307ff2114f299"
}
2025/02/03/[$LATEST]ea9a64ec87294bf6bbc9026c05a01e04 2025-02-03T14:59:51.126000 {
  "_aws": {
    "Timestamp": 1675436391126,
    "CloudWatchMetrics": [
      {
        "Namespace": "Powertools",
        "Dimensions": [
          [
            "function_name",
            "service"
          ]
        ],
        "Metrics": [
          {
            "Name": "ColdStart",
            "Unit": "Count"
          }
        ]
      }
    ]
  },
  "function_name": "sam-app-HelloWorldFunction-YBg8yfYtOc9j",
  "service": "PowertoolsHelloWorld",
  "ColdStart": [
    1.0
  ]
}
```

```
2025/02/03/[$LATEST]ea9a64ec87294bf6bbc9026c05a01e04 2025-02-03T14:59:51.126000 {
  "_aws": {
    "Timestamp": 1675436391126,
    "CloudWatchMetrics": [
      {
        "Namespace": "Powertools",
        "Dimensions": [
          [
            "service"
          ]
        ],
        "Metrics": [
          {
            "Name": "HelloWorldInvocations",
            "Unit": "Count"
          }
        ]
      }
    ]
  },
  "service": "PowertoolsHelloWorld",
  "HelloWorldInvocations": [
    1.0
  ]
}
2025/02/03/[$LATEST]ea9a64ec87294bf6bbc9026c05a01e04 2025-02-03T14:59:51.128000 END
 RequestId: d455cfc4-7704-46df-901b-2a5cce9405be
2025/02/03/[$LATEST]ea9a64ec87294bf6bbc9026c05a01e04 2025-02-03T14:59:51.128000
 REPORT RequestId: d455cfc4-7704-46df-901b-2a5cce9405be    Duration: 16.33 ms
 Billed Duration: 756 ms    Memory Size: 128 MB    Max Memory Used: 64 MB    Init
 Duration: 739.46 ms
XRAY TraceId: 1-63dd2166-434a12c22e1307ff2114f299    SegmentId: 3c5d18d735a1ced0
 Sampled: true
```

12. Il s’agit d’un point de terminaison d’API public accessible par Internet. Nous vous recommandons de supprimer le point de terminaison après un test.

```
cdk destroy
```

AWS Lambda Tests de fonctions événementielles en Python

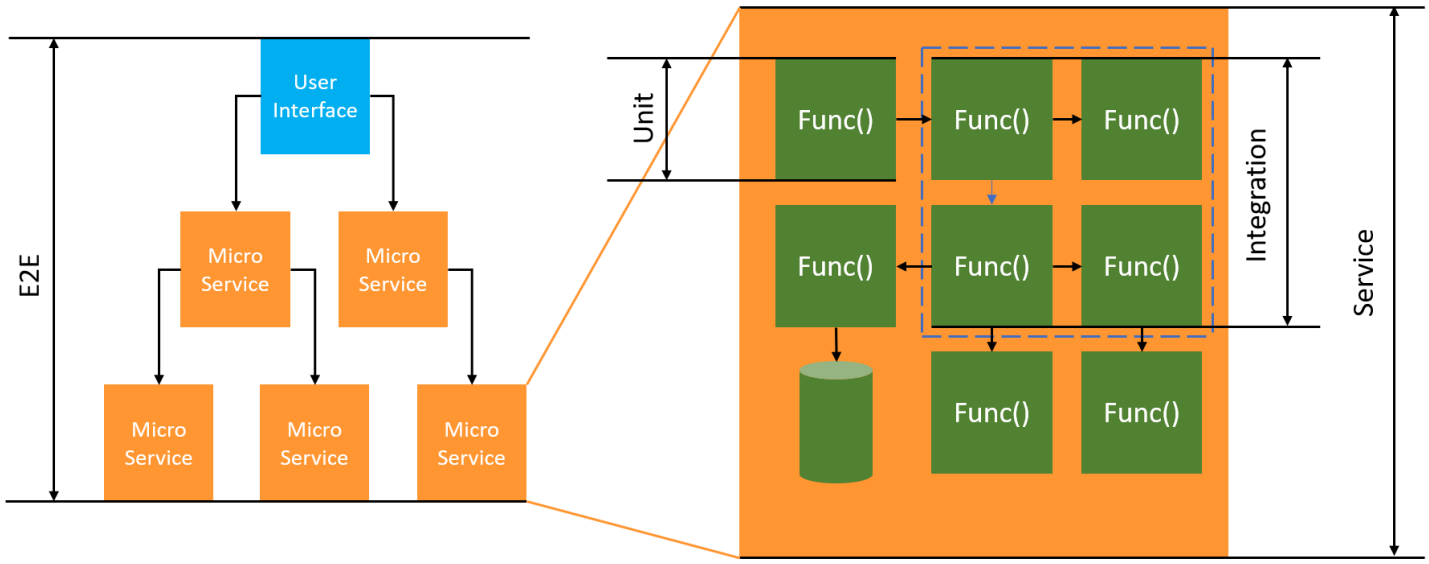
> **Note**
>
> Consultez le chapitre Test des fonctions pour une présentation complète des techniques et des bonnes pratiques pour tester les solutions sans serveur.

Le test des fonctions sans serveur utilise des types et des techniques de test traditionnels, mais vous devez également envisager de tester les applications sans serveur dans leur ensemble. Cloud-based les tests fournissent la mesure la plus précise de la qualité de vos fonctions et de vos applications sans serveur.

Une architecture d'application sans serveur comprend des services gérés qui fournissent des fonctionnalités d'applications critiques par le biais d'appels d'API. C'est pourquoi votre cycle de développement doit inclure des tests automatisés qui vérifient la fonctionnalité lorsque votre fonction et vos services interagissent.

Si vous ne créez pas de tests basés sur le cloud, vous pouvez rencontrer des problèmes en raison des différences entre votre environnement local et l'environnement déployé. Votre processus d'intégration continue doit exécuter des tests sur une série de ressources allouées dans le cloud avant de promouvoir votre code vers l'environnement de déploiement suivant, comme l'assurance qualité, la mise en place ou la production.

Poursuivez la lecture de ce petit guide pour en savoir plus sur les stratégies de test pour les applications sans serveur, ou rendez-vous sur le référentiel Serverless Test Samples pour vous plonger dans des exemples pratiques, spécifiques au langage et à l'exécution que vous avez choisis.



Pour les tests sans serveur, vous pouvez toujours écrire des tests unitaires, d'intégration et de bout en bout.

- Tests unitaires : tests exécutés sur un bloc de code isolé. Par exemple, la vérification de la logique métier permettant de calculer les frais de livraison en fonction d'un article et d'une destination donnés.
- Tests d'intégration : tests impliquant au moins deux composants ou services qui interagissent, généralement dans un environnement cloud. Par exemple, la vérification d'une fonction traite les événements d'une file d'attente.
- End-to-end tests - Tests qui vérifient le comportement dans l'ensemble d'une application. Il s'agit par exemple de s'assurer que l'infrastructure est correctement mise en place et que les événements circulent entre les services comme prévu pour enregistrer la commande d'un client.

Test de vos applications sans serveur

Vous utilisez généralement une combinaison d'approches pour tester le code de votre application sans serveur, notamment des tests dans le cloud, des tests avec des simulations et parfois des tests avec des émulateurs.

Tests dans le cloud

Les tests dans le cloud sont utiles pour toutes les phases des tests, y compris les tests unitaires, les tests d'intégration et les tests de bout en bout. Vous exécutez des tests sur du code déployé dans le cloud et interagissez avec des services basés sur le cloud. Cette approche fournit la mesure la plus précise de la qualité de votre code.

Un moyen pratique de déboguer votre fonction d'événement Lambda dans le cloud consiste à utiliser la console avec un événement de test. Un événement de test est une entrée JSON pour votre fonction. Si votre fonction ne nécessite pas d'entrée, l'événement peut être un document JSON vide (`{}`). La console fournit des exemples d'événements pour diverses intégrations de services. Après avoir créé un événement dans la console, vous pouvez le partager avec votre équipe pour faciliter les tests et les rendre plus cohérents.

> **Note**
>
> Tester une fonction dans la console est un moyen rapide de démarrer, mais l'automatisation de vos cycles de test garantit la qualité des applications et la rapidité du développement.

Outils de test

Il existe des outils et des techniques permettant d'accélérer les boucles de rétroaction du développement. Par exemple, AWS SAM Accelerate et le mode de surveillance AWS CDK réduisent tous deux le temps nécessaire à la mise à jour des environnements cloud.

Moto est une bibliothèque Python permettant de simuler AWS des services et des ressources, afin que vous puissiez tester vos fonctions avec peu ou pas de modifications à l'aide de décorateurs pour intercepter et simuler les réponses.

La fonctionnalité de validation de Powertools for AWS Lambda (Python) fournit des décorateurs qui vous permettent de valider les événements d'entrée et les réponses de sortie de vos fonctions Python.

Pour plus d'informations, consultez le billet de blog Unit Testing Lambda with Python and Mock AWS Services.

Pour réduire la latence associée aux itérations de déploiement dans le cloud, consultez AWS Serverless Application Model (AWS SAM) Accelerate, mode de AWS surveillance du Cloud Development Kit (AWS CDK). Ces outils surveillent les modifications apportées à votre infrastructure et à votre code. Ils réagissent à ces modifications en créant et en déployant automatiquement des mises à jour incrémentielles dans votre environnement cloud.

Des exemples utilisant ces outils sont disponibles dans le référentiel de code Python Test Samples.

Instrumentation du code Python dans AWS Lambda

Lambda s'intègre pour vous aider AWS X-Ray à suivre, à déboguer et à optimiser les applications Lambda. Vous pouvez l'utiliser X-Ray pour suivre une demande lorsqu'elle parcourt les ressources de votre application, ce qui peut inclure des fonctions Lambda et AWS d'autres services.

Pour envoyer des données de suivi à X-Ray, vous pouvez utiliser l'une des trois bibliothèques du SDK :

- AWS Distro for OpenTelemetry (ADOT) — Une distribution sécurisée, prête pour la production et prise AWS en charge du SDK (OTel). OpenTelemetry
- Kit SDK AWS X-Ray pour Python— Un SDK pour générer et envoyer des données de trace à X-Ray.
- Powertools for AWS Lambda (Python) — Une boîte à outils pour les développeurs permettant de mettre en œuvre les meilleures pratiques sans serveur et d'accroître la rapidité des développeurs.

Chacun des SDK propose des moyens d'envoyer vos données de télémétrie au service. X-Ray Vous pouvez ensuite les utiliser X-Ray pour afficher, filtrer et obtenir des informations sur les indicateurs de performance de votre application afin d'identifier les problèmes et les opportunités d'optimisation.

> **Important**
>
> Les X-Ray et Powertools for AWS Lambda SDK font partie d'une solution d'instrumentation étroitement intégrée proposée par. AWS Les couches ADOT Lambda font partie d'une norme industrielle pour l'instrumentation de traçage qui collecte plus de données en général, mais qui peut ne pas convenir à tous les cas d'utilisation. Vous pouvez implémenter le suivi de bout en bout à l' X-Ray aide de l'une ou l'autre solution. Pour en savoir plus sur le choix entre les deux, voir Choisir entre la AWS distribution pour Open Telemetry et les SDK. X-Ray

Sections

- Utilisation de Powertools pour AWS Lambda (Python) et AWS SAM pour le traçage
- Utilisation de Powertools pour AWS Lambda (Python) et le AWS CDK pour le traçage
- Utilisation d'ADOT pour instrumenter vos fonctions python
- Utiliser le X-Ray SDK pour instrumenter vos fonctions Python
- Activation du suivi avec la console Lambda

- Activation du suivi avec l'API Lambda
- Activation du traçage avec CloudFormation
- Interprétation et X-Ray traçage
- Stockage des dépendances d'exécution dans une couche (X-Ray SDK)

Utilisation de Powertools pour AWS Lambda (Python) et AWS SAM pour le traçage

Suivez les étapes ci-dessous pour télécharger, créer et déployer un exemple d'application Hello World Python avec des modules Powertools pour AWS Lambda (Python) intégrés à l'aide du AWS SAM. Cette application met en œuvre un backend API de base et utilise Powertools pour émettre des journaux, des métriques et des traces. Il se compose d'un point de terminaison Amazon API Gateway et d'une fonction d'événement Lambda. Lorsque vous envoyez une requête GET au point de terminaison API Gateway, la fonction invoque, envoie des journaux et des métriques à l'aide du format métrique intégré à CloudWatch, et envoie des traces à AWS X-Ray. La fonction renvoie un message hello world.

Conditions préalables

Pour exécuter la procédure indiquée dans cette section, vous devez satisfaire aux exigences suivantes :

- Python 3.11
- AWS CLI version 2
- AWS SAM CLI version 1.75 ou ultérieure. Si vous disposez d'une ancienne version de la AWS SAM CLI, consultez la section Mise à niveau de la AWS SAM CLI.

Déployer un échantillon AWS SAM vigie

1. Initialisez l'application à l'aide du modèle Hello World Python.

```
sam init --app-template hello-world-powertools-python --name sam-app --package-type
 Zip --runtime python3.11 --no-tracing
```

2. Créez l'application.

```
cd sam-app && sam build
```

3. Déployez l'application.

```
sam deploy --guided
```

4. Suivez les invites à l'écran. Appuyez sur `Enter` pour accepter les options par défaut fournies dans l'expérience interactive.

> **Note**
>
> Car l'autorisation n'a HelloWorldFunction peut-être pas été définie, est-ce que ça va ? , assurez-vous de participery.

5. Obtenez l'URL de l'application déployée :

```
aws cloudformation describe-stacks --stack-name sam-app --query
 'Stacks[0].Outputs[?OutputKey==`HelloWorldApi`].OutputValue' --output text
```

6. Invoquez le point de terminaison de l'API :

```
curl -X GET <URL_FROM_PREVIOUS_STEP>
```

En cas de succès, vous obtiendrez cette réponse :

```
{"message":"hello world"}
```

7. Pour obtenir les traces de la fonction, exécutez sam traces.

```
sam traces
```

La sortie de la trace ressemble à ceci :

```
New XRay Service Graph
  Start time: 2023-02-03 14:59:50+00:00
  End time: 2023-02-03 14:59:50+00:00
  Reference Id: 0 - (Root) AWS::Lambda - sam-app-HelloWorldFunction-YBg8yfYtOc9j -
 Edges: [1]
   Summary_statistics:
     - total requests: 1
     - ok count(2XX): 1
     - error count(4XX): 0
     - fault count(5XX): 0
```

```
      - total response time: 0.924
   Reference Id: 1 - AWS::Lambda::Function - sam-app-HelloWorldFunction-YBg8yfYtOc9j
  - Edges: []
    Summary_statistics:
      - total requests: 1
      - ok count(2XX): 1
      - error count(4XX): 0
      - fault count(5XX): 0
      - total response time: 0.016
   Reference Id: 2 - client - sam-app-HelloWorldFunction-YBg8yfYtOc9j - Edges: [0]
    Summary_statistics:
      - total requests: 0
      - ok count(2XX): 0
      - error count(4XX): 0
      - fault count(5XX): 0
      - total response time: 0

XRay Event [revision 1] at (2023-02-03T14:59:50.204000) with id
 (1-63dd2166-434a12c22e1307ff2114f299) and duration (0.924s)
 - 0.924s - sam-app-HelloWorldFunction-YBg8yfYtOc9j [HTTP: 200]
 - 0.016s - sam-app-HelloWorldFunction-YBg8yfYtOc9j
   - 0.739s - Initialization
   - 0.016s - Invocation
     - 0.013s - ## lambda_handler
       - 0.000s - ## app.hello
   - 0.000s - Overhead
```

8. Il s’agit d’un point de terminaison d’API public accessible par Internet. Nous vous recommandons de supprimer le point de terminaison après un test.

```
sam delete
```

X-Ray ne retrace pas toutes les demandes jusqu'à votre application. X-Ray applique un algorithme d'échantillonnage pour garantir l'efficacité du suivi, tout en fournissant un échantillon représentatif de toutes les demandes. Le taux d’échantillonnage est 1 demande par seconde et 5 % de demandes supplémentaires. Vous ne pouvez pas configurer le taux X-Ray d'échantillonnage pour vos fonctions.

Utilisation de Powertools pour AWS Lambda (Python) et le AWS CDK pour le traçage

Suivez les étapes ci-dessous pour télécharger, créer et déployer un exemple d'application Hello World Python avec des modules Powertools pour AWS Lambda (Python) intégrés à l'aide du AWS

CDK. Cette application met en œuvre un backend API de base et utilise Powertools pour émettre des journaux, des métriques et des traces. Il se compose d'un point de terminaison Amazon API Gateway et d'une fonction d'événement Lambda. Lorsque vous envoyez une requête GET au point de terminaison API Gateway, la fonction invoque, envoie des journaux et des métriques à l'aide du format métrique intégré à CloudWatch, et envoie des traces à AWS X-Ray. La fonction renvoie un message hello world.

Conditions préalables

Pour exécuter la procédure indiquée dans cette section, vous devez satisfaire aux exigences suivantes :

- Python 3.11
- AWS CLI version 2
- AWS CDK version 2
- AWS SAM CLI version 1.75 ou ultérieure. Si vous disposez d'une ancienne version de la AWS SAM CLI, consultez la section Mise à niveau de la AWS SAM CLI.

Déployer un échantillon AWS CDK vigie

1. Créez un répertoire de projets pour votre nouvelle application.

```
mkdir hello-world
cd hello-world
```

2. Initialisez l’application.

```
cdk init app --language python
```

3. Installez les dépendances de Python.

```
pip install -r requirements.txt
```

4. Créez un répertoire lambda_function dans le dossier racine.

```
mkdir lambda_function
cd lambda_function
```

5. Créez un fichier app.py et ajoutez-y le code suivant. Il s'agit du code de la fonction .

```
from aws_lambda_powertools.event_handler import APIGatewayRestResolver
from aws_lambda_powertools.utilities.typing import LambdaContext
from aws_lambda_powertools.logging import correlation_paths
from aws_lambda_powertools import Logger
from aws_lambda_powertools import Tracer
from aws_lambda_powertools import Metrics
from aws_lambda_powertools.metrics import MetricUnit

app = APIGatewayRestResolver()
tracer = Tracer()
logger = Logger()
metrics = Metrics(namespace="PowertoolsSample")

@app.get("/hello")
@tracer.capture_method
def hello():
    # adding custom metrics
    # See: https://docs.powertools.aws.dev/lambda-python/latest/core/metrics/
    metrics.add_metric(name="HelloWorldInvocations", unit=MetricUnit.Count,
 value=1)

    # structured log
    # See: https://docs.powertools.aws.dev/lambda-python/latest/core/logger/
    logger.info("Hello world API - HTTP 200")
    return {"message": "hello world"}

# Enrich logging with contextual information from Lambda
@logger.inject_lambda_context(correlation_id_path=correlation_paths.API_GATEWAY_REST)
# Adding tracer
# See: https://docs.powertools.aws.dev/lambda-python/latest/core/tracer/
@tracer.capture_lambda_handler
# ensures metrics are flushed upon request completion/failure and capturing
 ColdStart metric
@metrics.log_metrics(capture_cold_start_metric=True)
def lambda_handler(event: dict, context: LambdaContext) -> dict:
    return app.resolve(event, context)
```

6. Ouvrez le répertoire hello_world. Vous devriez voir un fichier nommé hello_world_stack.py.

```
cd ..
cd hello_world
```

7. Ouvrez hello_world_stack.py et ajoutez le code suivant au fichier. Il contient le constructeur Lambda, qui crée la fonction, configure les variables d'environnement pour Powertools et définit la durée de conservation des journaux à une semaine, et le constructeur ApiGatewayv 1, qui crée l'API REST.

```
from aws_cdk import (
    Stack,
    aws_apigateway as apigwv1,
    aws_lambda as lambda_,
    CfnOutput,
    Duration
)
from constructs import Construct

class HelloWorldStack(Stack):

    def __init__(self, scope: Construct, construct_id: str, **kwargs) -> None:
        super().__init__(scope, construct_id, **kwargs)

        # Powertools Lambda Layer
        powertools_layer = lambda_.LayerVersion.from_layer_version_arn(
            self,
            id="lambda-powertools",
            # At the moment we wrote this example, the aws_lambda_python_alpha CDK
 constructor is in Alpha, o we use layer to make the example simpler
            # See https://docs.aws.amazon.com/cdk/api/v2/python/
aws_cdk.aws_lambda_python_alpha/README.html
            # Check all Powertools layers versions here: https://
docs.powertools.aws.dev/lambda-python/latest/#lambda-layer
            layer_version_arn=f"arn:aws:lambda:
{self.region}:017000801446:layer:AWSLambdaPowertoolsPythonV2:21"
        )

        function = lambda_.Function(self,
            'sample-app-lambda',
            runtime=lambda_.Runtime.PYTHON_3_11,
            layers=[powertools_layer],
            code = lambda_.Code.from_asset("./lambda_function/"),
            handler="app.lambda_handler",
            memory_size=128,
            timeout=Duration.seconds(3),
            architecture=lambda_.Architecture.X86_64,
            environment={
```

```
                "POWERTOOLS_SERVICE_NAME": "PowertoolsHelloWorld",
                "POWERTOOLS_METRICS_NAMESPACE": "PowertoolsSample",
                "LOG_LEVEL": "INFO"
            }
        )

        apigw = apigwv1.RestApi(self, "PowertoolsAPI",
 deploy_options=apigwv1.StageOptions(stage_name="dev"))

        hello_api = apigw.root.add_resource("hello")
        hello_api.add_method("GET", apigwv1.LambdaIntegration(function,
 proxy=True))

        CfnOutput(self, "apiUrl", value=f"{apigw.url}hello")
```

8. Déployez votre application.

```
cd ..
cdk deploy
```

9. Obtenez l'URL de l'application déployée :

```
aws cloudformation describe-stacks --stack-name HelloWorldStack --query
 'Stacks[0].Outputs[?OutputKey==`apiUrl`].OutputValue' --output text
```

10. Invoquez le point de terminaison de l'API :

```
curl -X GET <URL_FROM_PREVIOUS_STEP>
```

    En cas de succès, vous obtiendrez cette réponse :

```
{"message":"hello world"}
```

11. Pour obtenir les traces de la fonction, exécutez sam traces.

```
sam traces
```

    La sortie des traces ressemble à ceci :

```
New XRay Service Graph
  Start time: 2023-02-03 14:59:50+00:00
  End time: 2023-02-03 14:59:50+00:00
```

```
  Reference Id: 0 - (Root) AWS::Lambda - sam-app-HelloWorldFunction-YBg8yfYtOc9j -
 Edges: [1]
   Summary_statistics:
     - total requests: 1
     - ok count(2XX): 1
     - error count(4XX): 0
     - fault count(5XX): 0
     - total response time: 0.924
  Reference Id: 1 - AWS::Lambda::Function - sam-app-HelloWorldFunction-YBg8yfYtOc9j
 - Edges: []
   Summary_statistics:
     - total requests: 1
     - ok count(2XX): 1
     - error count(4XX): 0
     - fault count(5XX): 0
     - total response time: 0.016
  Reference Id: 2 - client - sam-app-HelloWorldFunction-YBg8yfYtOc9j - Edges: [0]
   Summary_statistics:
     - total requests: 0
     - ok count(2XX): 0
     - error count(4XX): 0
     - fault count(5XX): 0
     - total response time: 0

XRay Event [revision 1] at (2023-02-03T14:59:50.204000) with id
 (1-63dd2166-434a12c22e1307ff2114f299) and duration (0.924s)
 - 0.924s - sam-app-HelloWorldFunction-YBg8yfYtOc9j [HTTP: 200]
 - 0.016s - sam-app-HelloWorldFunction-YBg8yfYtOc9j
   - 0.739s - Initialization
   - 0.016s - Invocation
     - 0.013s - ## lambda_handler
       - 0.000s - ## app.hello
   - 0.000s - Overhead
```

12. Il s’agit d’un point de terminaison d’API public accessible par Internet. Nous vous recommandons de supprimer le point de terminaison après un test.

```
cdk destroy
```

Utilisation d'ADOT pour instrumenter vos fonctions python

ADOT fournit des couches Lambda entièrement gérées qui regroupent tout ce dont vous avez besoin pour collecter des données de télémétrie à l'aide du kit SDK OTel. En consommant cette couche, vous pouvez instrumenter vos fonctions Lambda sans avoir à modifier le code de fonction. Vous pouvez également configurer votre couche pour effectuer une initialisation personnalisée d'OTel. Pour de plus amples informations, veuillez consulter Configuration personnalisée pour ADOT Collector sur Lambda dans la documentation ADOT.

Pour les exécutions python, vous pouvez ajouter leAWS couche Lambda gérée pour ADOT Pythonpour instrumenter automatiquement vos fonctions. Cette couche fonctionne à la fois pour les architectures arm64 et x86_64. Pour des instructions détaillées sur la façon d'ajouter cette couche, consultez AWS Distro for OpenTelemetry Lambda Support for Python dans la documentation ADOT.

Utiliser le X-Ray SDK pour instrumenter vos fonctions Python

Pour enregistrer les détails des appels que votre fonction effectue vers d'autres ressources de votre application, vous pouvez également utiliser le Kit SDK AWS X-Ray pour Python. Pour obtenir ce kit SDK, ajoutez le package `aws-xray-sdk` aux dépendances de votre application.

Example requirements.txt

```
jsonpickle==1.3
aws-xray-sdk==2.4.3
```

Dans votre code de fonction, vous pouvez instrumenter les clients du AWS SDK en appliquant un correctif à la `boto3` bibliothèque avec le `aws_xray_sdk.core` module.

Example function — Tracer un AWS Client du SDK

```
import boto3
from aws_xray_sdk.core import xray_recorder
from aws_xray_sdk.core import patch_all

logger = logging.getLogger()
logger.setLevel(logging.INFO)
patch_all()

client = boto3.client('lambda')
client.get_account_settings()
```

```
def lambda_handler(event, context):
    logger.info('## ENVIRONMENT VARIABLES\r' + jsonpickle.encode(dict(**os.environ)))
  ...
```

Après avoir ajouté les bonnes dépendances et apporté les modifications de code nécessaires, activez le suivi dans la configuration de votre fonction via la console Lambda ou l'API.

Activation du suivi avec la console Lambda

Pour activer le suivi actif de votre fonction d'événement Lambda à l'aide de la console, procédez comme suit :

Pour activer le traçage actif

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez une fonction d'événement.
3. Choisissez Configuration, puis choisissez Outils de surveillance et d’opérations.
4. Dans Outils de surveillance supplémentaires, choisissez Modifier.
5. Sous Signaux CloudWatch d'application et AWS X-Ray sélectionnez Activer les traces de service Lambda.
6. Cliquez sur Enregistrer.

Activation du suivi avec l’API Lambda

Configurez le suivi sur votre fonction Lambda avec le AWS SDK AWS CLI or, utilisez les opérations d'API suivantes :

- UpdateFunctionConfiguration
- GetFunctionConfiguration
- CreateFunction

L'exemple de AWS CLI commande suivant active le suivi actif sur une fonction nommée my-function.

```
aws lambda update-function-configuration --function-name my-function \
--tracing-config Mode=Active
```

Le mode de suivi fait partie de la configuration spécifique de la version lorsque vous publiez une version de votre fonction. Vous ne pouvez pas modifier le mode de suivi sur une version publiée.

Activation du traçage avec CloudFormation

Pour activer le suivi d'une `AWS::Lambda::Function` ressource dans un CloudFormation modèle, utilisez la `TracingConfig` propriété.

Example fonction-inline.yml — Configuration du suivi

```
Resources:
  function:
    Type: AWS::Lambda::Function
    Properties:
      TracingConfig:
        Mode: Active
      ...
```

Pour une `AWS::Serverless::Function` ressource AWS Serverless Application Model (AWS SAM), utilisez la `Tracing` propriété.

Example template.yml — Configuration du suivi

```
Resources:
  function:
    Type: AWS::Serverless::Function
    Properties:
      Tracing: Active
      ...
```

Interprétation et X-Ray traçage

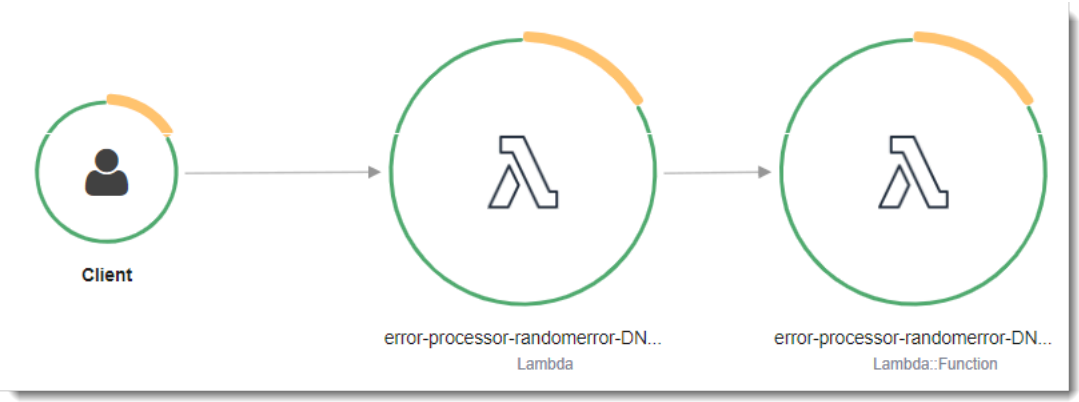
Votre fonction événementielle a besoin d'une autorisation pour télécharger des données de suivi sur X-Ray. Lorsque vous activez le suivi dans la console Lambda, Lambda ajoute les autorisations requises au rôle d'exécution de votre fonction d'événement. Dans le cas contraire, ajoutez la AWSXRayDaemonWriteAccesspolitique au rôle d'exécution.

Une fois que vous avez configuré le suivi actif, vous pouvez observer des demandes spécifiques via votre application. Le graphique X-Ray de service affiche des informations sur votre application et tous ses composants. L'exemple suivant montre une application dotée de deux fonctions. La fonction

principale traite les événements et renvoie parfois des erreurs. La deuxième fonction située en haut traite les erreurs qui apparaissent dans le groupe de journaux de la première et utilise le AWS SDK pour appeler X-Ray Amazon Simple Storage Service (Amazon S3) et Amazon Logs. CloudWatch

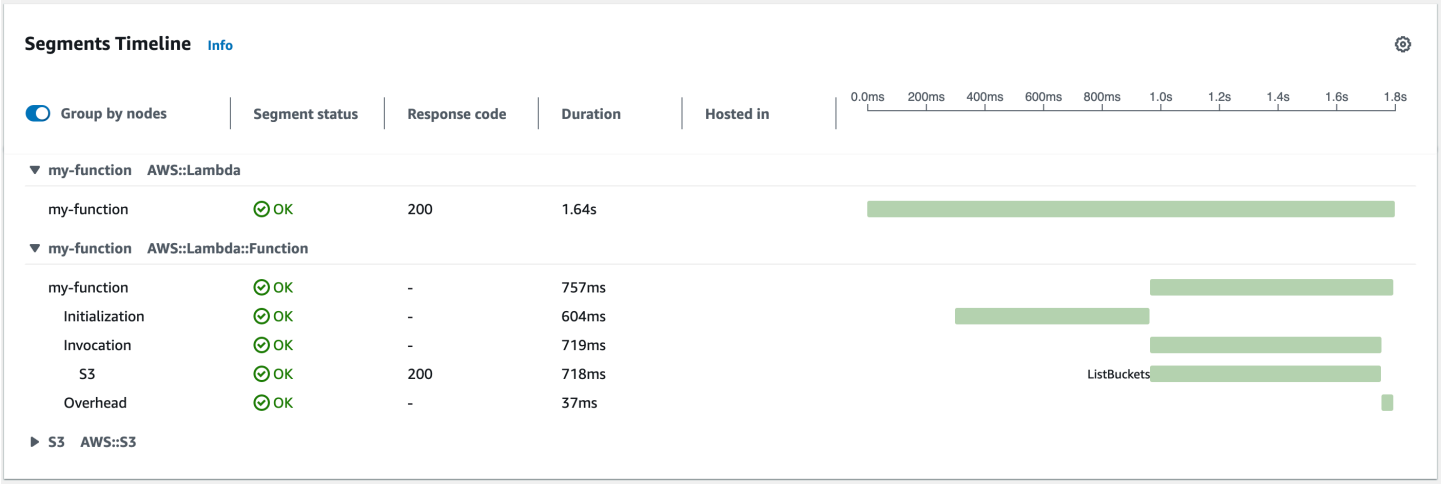
X-Ray ne retrace pas toutes les demandes jusqu'à votre application. X-Ray applique un algorithme d'échantillonnage pour garantir l'efficacité du suivi, tout en fournissant un échantillon représentatif de toutes les demandes. Le taux d'échantillonnage est 1 demande par seconde et 5 % de demandes supplémentaires. Vous ne pouvez pas configurer le taux X-Ray d'échantillonnage pour vos fonctions.

Dans X-Ray, un suivi enregistre des informations relatives à une demande traitée par un ou plusieurs services. Lambda enregistre deux segments par suivi, ce qui a pour effet de créer deux nœuds sur le graphique du service. L'image suivante met en évidence ces deux nœuds :



Le premier nœud sur la gauche représente le service Lambda qui reçoit la demande d'invocation. Le deuxième nœud représente votre fonction Lambda spécifique. L'exemple suivant illustre une trace avec ces deux segments. Les deux sont nommés my-function, mais l'un a pour origine `AWS::Lambda` et l'autre a pour origine `AWS::Lambda::Function`. Si le segment `AWS::Lambda`

affiche une erreur, cela signifie que le service Lambda a rencontré un problème. Si le segment `AWS::Lambda::Function` affiche une erreur, cela signifie que votre fonction a rencontré un problème.



Cet exemple développe le segment `AWS::Lambda::Function` pour afficher ses trois sous-segments.

> **Note**
>
> AWS met actuellement en œuvre des modifications du service Lambda. En raison de ces modifications, vous pouvez constater des différences mineures entre la structure et le contenu des messages du journal système et des segments de trace émis par les différentes fonctions d'événement Lambda de votre ordinateur. Compte AWS
> L'exemple de suivi présenté ici illustre le segment de fonction à l'ancienne. Les différences entre les segments à l'ancienne et de style moderne sont décrites dans les paragraphes suivants.
> Ces modifications seront mises en œuvre au cours des prochaines semaines, et toutes les fonctions, Régions AWS sauf en Chine et dans les GovCloud régions, seront transférées pour utiliser le nouveau format des messages de journal et des segments de trace.

Le segment de fonction à l'ancienne contient les sous-segments suivants :

- Initialization (Initialisation) : représente le temps passé à charger votre fonction et à exécuter le code d'initialisation. Ce sous-segment apparaît pour le premier événement traité par chaque instance de votre fonction.
- Invocation – Représente le temps passé à exécuter votre code de gestionnaire.

- Overhead (Travail supplémentaire) – Représente le temps que le fichier d'exécution Lambda passe à se préparer à gérer l'événement suivant.

Le segment de fonction de style moderne ne contient pas de sous-segment `Invocation`. À la place, les sous-segments du client sont directement rattachés au segment de fonction. Pour plus d'informations sur la structure des segments de fonction à l'ancienne et de style moderne, consultez the section called "Comprendre les X-Ray traces".

Vous pouvez également utiliser des clients HTTP, enregistrer des requêtes SQL et créer des sous-segments personnalisés avec des annotations et des métadonnées. Pour plus d'informations, consultez Kit SDK AWS X-Ray pour Python dans le AWS X-Ray Guide du développeur.

> **Tarification**
>
> Vous pouvez utiliser le X-Ray suivi gratuitement chaque mois jusqu'à une certaine limite dans le cadre du niveau AWS gratuit. Au-delà de ce seuil, les X-Ray frais de stockage et de récupération des traces sont facturés. Pour en savoir plus, consultez Pricing AWS X-Ray (Tarification).

Stockage des dépendances d'exécution dans une couche (X-Ray SDK)

Si vous utilisez le X-Ray SDK pour instrumenter le code de fonction des clients du AWS SDK, votre package de déploiement peut devenir assez volumineux. Pour éviter de télécharger les dépendances d'exécution chaque fois que vous mettez à jour le code de votre fonction, empaquetez le X-Ray SDK dans une couche Lambda.

L'exemple suivant montre une ressource `AWS::Serverless::LayerVersion` qui stocke le Kit SDK AWS X-Ray pour Python.

Example template.yml — Couche de dépendances

```
Resources:
  function:
    Type: AWS::Serverless::Function
    Properties:
      CodeUri: function/.
      Tracing: Active
      Layers:
```

```
        - !Ref libs
      ...
  libs:
    Type: AWS::Serverless::LayerVersion
    Properties:
      LayerName: blank-python-lib
      Description: Dependencies for the blank-python sample app.
      ContentUri: package/.
      CompatibleRuntimes:
        - python3.11
```

Avec cette configuration, vous ne mettez à jour les fichiers de couche de bibliothèque que si vous modifiez vos dépendances d'exécution. Étant donné que le package de déploiement de la fonction contient uniquement votre code, cela peut contribuer à réduire les temps de chargement.

La création d'une couche pour les dépendances nécessite des modifications de construction pour générer l'archive de couches avant le déploiement. Pour un exemple fonctionnel, consultez l'exemple d'application blank-python.

Création de fonctions d'événement Lambda avec Ruby

Vous pouvez exécuter du code Ruby dans AWS Lambda Event Functions. Lambda fournit des runtimes pour Ruby qui exécutent votre code afin de traiter des événements. Votre code s'exécute dans un environnement qui inclut le AWS SDK pour Ruby, avec les informations d'identification d'un rôle Gestion des identités et des accès AWS (IAM) que vous gérez. Pour en savoir plus sur les versions du kit SDK incluses dans les environnements d'exécution Ruby, consultez the section called "Runtime-included Versions du SDK".

Lambda prend en charge les runtimes Ruby suivants.

Nom	Identifiant	Système d'exploitation	Date d'obsolescence	Créer la fonction de blocage	Mettre à jour la fonction de blocage
Ruby 4.0	`ruby4.0`	Amazon Linux 2	31 mars 2029	30 avril 2029	31 mai 2029
Ruby 3.4	`ruby3.4`	Amazon Linux 2	31 mars 2028	30 avril 2028	31 mai 2028
Ruby 3.3	`ruby3.3`	Amazon Linux 2	31 mars 2027	29 juillet 2027	31 août 2027

Pour créer une fonction d'événement Ruby

1. Ouvrez la console Lambda.
2. Choisissez Create Event Function.
3. Configurez les paramètres suivants :
   - Nom de la fonction : saisissez le nom de la fonction.
   - Runtime : choisissez Ruby 4.0.
4. Choisissez Create Event Function.

La console crée une fonction d'événement Lambda avec un seul fichier source nommé. `lambda_function.rb` Vous pouvez modifier ce fichier et ajouter d'autres fichiers dans l'éditeur de code intégré. Dans la section DÉPLOYER, choisissez Déployer pour mettre à jour le code de votre fonction. Ensuite, pour exécuter votre code, choisissez Créer un événement de test dans la section ÉVÉNEMENTS DE TEST.

Le fichier `lambda_function.rb` exporte une fonction nommée `lambda_handler` qui accepte un objet événement et un objet contexte. Il s'agit de la fonction de gestionnaire que Lambda appelle lors de l'invocation de la fonction. Le runtime Ruby Event Function obtient les événements d'invocation de Lambda et les transmet au gestionnaire. Dans la configuration de fonction, la valeur de gestionnaire est `lambda_function.lambda_handler`.

Lorsque vous enregistrez votre code de fonction, la console Lambda crée un package de déploiement d'archive de fichiers .zip. Lorsque vous développez votre code de fonction en dehors de la console (à l'aide d'un IDE), vous devez créer un package de déploiement pour charger votre code dans la fonction Lambda.

Le runtime de la fonction transmet un objet de contexte au gestionnaire, en plus de l'événement d'invocation. L'objet de contexte contient des informations supplémentaires sur l'invocation, la fonction et l'environnement d'exécution. Des informations supplémentaires sont disponibles dans les variables d'environnement.

Votre fonction Lambda est fournie avec un groupe de CloudWatch journaux Logs. La fonction runtime envoie les détails de chaque appel à CloudWatch Logs. Il relaie tous les journaux que votre fonction génère pendant l'invocation. Si votre fonction renvoie une erreur, Lambda met en forme l'erreur et la renvoie à l'appelant.

Rubriques

- Runtime-included Versions du SDK
- Activer un autre JIT Ruby (YJIT)
- Définir le gestionnaire de fonctions d'événement Lambda dans Ruby
- Déployez les fonctions d'événement Ruby Lambda avec des archives de fichiers .zip
- Déployez les fonctions d'événement Ruby Lambda avec des images de conteneur
- Utilisation de couches pour les fonctions d'événement Ruby Lambda
- Utilisation de l'objet de contexte Lambda pour récupérer les informations de la fonction d'événement Ruby
- Enregistrez et surveillez les fonctions d'événements Ruby Lambda
- Instrumentation du code Ruby dans AWS Lambda

Runtime-included Versions du SDK

La version du AWS SDK incluse dans le runtime Ruby dépend de la version d'exécution et de votre Région AWS. Le AWS SDK pour Ruby est conçu pour être modulaire et est séparé par Service AWS. Pour trouver le numéro de version d'une gemme de service particulière incluse dans le moteur d'exécution que vous utilisez, créez une fonction d'événement Lambda avec un code au format suivant. Remplacez `aws-sdk-s3` et `Aws::S3` par le nom des gems de service utilisés par votre code.

```
require 'aws-sdk-s3'

def lambda_handler(event:, context:)
  puts "Service gem version: #{Aws::S3::GEM_VERSION}"
  puts "Core version: #{Aws::CORE_GEM_VERSION}"
end
```

Activer un autre JIT Ruby (YJIT)

Les environnements d'exécution Ruby supportent YJIT, un compilateur Ruby JIT léger et minimaliste. YJIT offre des performances nettement supérieures, mais utilise également plus de mémoire que l'interpréteur Ruby. YJIT est recommandé pour les charges de travail Ruby on Rails.

YJIT n'est pas activé par défaut. Pour activer YJIT pour une fonction Ruby, définissez la variable d'`RUBY_YJIT_ENABLE`environnement sur`1`. Pour confirmer que YJIT est activé, imprimez le résultat de la méthode `RubyVM::YJIT.enabled?`.

Example– Confirmez que YJIT est activé

```
puts(RubyVM::YJIT.enabled?())
# => true
```

Définir le gestionnaire de fonctions d'événement Lambda dans Ruby

Le gestionnaire de fonctions d'événement Lambda est la méthode de votre code de fonction qui traite les événements. Lorsque votre fonction est invoquée, Lambda exécute la méthode du gestionnaire. Votre fonction s'exécute jusqu'à ce que le gestionnaire renvoie une réponse, se ferme ou expire.

Rubriques

- Notions de base sur le gestionnaire Ruby
- Meilleures pratiques en matière de code pour les fonctions d'événement Ruby Lambda

Notions de base sur le gestionnaire Ruby

Dans l'exemple suivant, le fichier `function.rb` définit une méthode de gestionnaire nommée `handler`. La fonction de gestionnaire prend deux objets en tant qu'entrées et renvoie un document JSON.

Example function.rb

```
require 'json'

def handler(event:, context:)
    { event: JSON.generate(event), context: JSON.generate(context.inspect) }
end
```

Dans la configuration de votre fonction, le paramètre `handler` indique à Lambda où trouver le gestionnaire. Pour l'exemple précédent, la valeur correcte pour ce paramètre est **`function.handler`**. Elle inclut deux noms séparées par un point : le nom du fichier et le nom de la méthode de gestionnaire.

Vous pouvez également définir votre méthode de gestionnaire dans une classe. L'exemple suivant définit une méthode de gestionnaire nommée `process` sur une classe nommée `Handler` dans un module appelé `LambdaFunctions`.

Example source.rb

```
module LambdaFunctions
  class Handler
    def self.process(event:,context:)
      "Hello!"
```

```
    end
  end
end
```

Dans ce cas, le paramètre de gestionnaire est **`source.LambdaFunctions::Handler.process`**.

Les deux objets qui sont acceptés par le gestionnaire sont l'événement d'invocation et le contexte. L'événement est un objet Ruby qui contient la charge utile qui est fournie par le mécanisme d'invocation. Si la charge utile est un document JSON, l'objet d'événement est un hachage Ruby. Sinon, il s'agit d'une chaîne. L'objet de contexte contient des méthodes et des propriétés qui fournissent des informations sur l'invocation, la fonction et l'environnement d'exécution.

Le gestionnaire de fonction est exécuté chaque fois que votre fonction Lambda est invoquée. Le code statique à l'extérieur du gestionnaire est exécuté une fois par instance de la fonction. Si votre gestionnaire utilise des ressources telles que les clients de kits SDK et les connexions de base de données, vous pouvez les créer à l'extérieur de la méthode de gestionnaire afin de les réutiliser pour plusieurs invocations.

Chaque instance de votre fonction peut traiter plusieurs événements d'invocations, mais elle ne traite qu'un événement à la fois. Le nombre d'instances traitant un événement à un moment donné est la simultanéité de votre fonction. Pour plus d'informations sur l'environnement d'exécution Lambda, consultez Comprendre le cycle de vie de l'environnement d'exécution Lambda.

Meilleures pratiques en matière de code pour les fonctions d'événement Ruby Lambda

Respectez les directives de la liste suivante pour utiliser les pratiques exemplaires de codage lors de la création de vos fonctions Lambda :

- Séparez le gestionnaire Lambda de votre logique principale. Cela facilite la création d'une fonction plus testable à l'unité. Par exemple, dans Ruby, cela peut ressembler à ceci :

```
def lambda_handler(event:, context:)
    foo = event['foo']
    bar = event['bar']

    result = my_lambda_function(foo:, bar:)

end

def my_lambda_function(foo:, bar:)
    // MyLambdaFunction logic here
```

```
end
```

- Contrôlez les dépendances du package de déploiement de vos fonctions. L'environnement d'exécution AWS Lambda contient un certain nombre de bibliothèques. Pour le runtime Ruby, il s'agit notamment du AWS SDK.

  Pour activer les dernières fonctionnalités et mises à jour de sécurité, Lambda met régulièrement à jour ces bibliothèques. Ces mises à jour peuvent apporter des modifications subtiles au comportement de votre fonction Lambda. Pour disposer du contrôle total des dépendances que votre fonction utilise, empaquetez toutes vos dépendances avec votre package de déploiement.
- Réduisez la complexité de vos dépendances. Privilégiez les infrastructures plus simples qui se chargent rapidement au démarrage de l'environnement d'exécution.
- Réduisez la taille de votre package de déploiement selon ses besoins d'exécution. Cela réduit le temps nécessaire au téléchargement et au déballage de votre package de déploiement avant l'invocation. Pour les fonctions créées dans Ruby, évitez de télécharger l'intégralité de la bibliothèque du AWS SDK dans le cadre de votre package de déploiement. Dépendez plutôt de manière sélective des gemmes qui récupèrent les composants du SDK dont vous avez besoin (par exemple, les gemmes du SDK DynamoDB ou Amazon S3).

Tirez parti de la réutilisation de l'environnement d'exécution pour améliorer les performances de votre fonction. Initialisez les clients SDK et les connexions à la base de données en dehors du gestionnaire de fonctions et mettez en cache les actifs statiques localement dans le répertoire `/tmp`. Les invocations ultérieures traitées par la même instance de votre fonction peuvent réutiliser ces ressources. Cela permet d'économiser des coûts, tout en réduisant le temps d'exécution de la fonction.

Pour éviter des éventuelles fuites de données entre les invocations, n'utilisez pas l'environnement d'exécution pour stocker des données utilisateur, des événements ou d'autres informations ayant un impact sur la sécurité. Si votre fonction repose sur un état réversible qui ne peut pas être stocké en mémoire dans le gestionnaire, envisagez de créer une fonction distincte ou des versions distinctes d'une fonction pour chaque utilisateur.

Utilisez une directive keep-alive pour maintenir les connexions persistantes. Lambda purge les connexions inactives au fil du temps. Si vous tentez de réutiliser une connexion inactive lorsque vous invoquez une fonction, cela entraîne une erreur de connexion. Pour maintenir votre connexion persistante, utilisez la directive Keep-alive associée à votre environnement d'exécution. Pour un exemple, voir Réutilisation des connexions avec Keep-Alive in Node.js.

Utilisez des variables d'environnement pour transmettre des paramètres opérationnels à votre fonction. Par exemple, si vous écrivez dans un compartiment Amazon S3 au lieu de coder en dur le nom du compartiment dans lequel vous écrivez, configurez le nom du compartiment comme variable d'environnement.

Évitez d'utiliser des invocations récursives dans votre fonction Lambda, lorsque la fonction s'invoque elle-même ou démarre un processus susceptible de l'invoquer à nouveau. Cela peut entraîner un volume involontaire d'invocations de fonction et des coûts accrus. Si vous constatez un volume involontaire d'invocations, définissez immédiatement la simultanéité réservée à la fonction sur `0` afin de limiter toutes les invocations de la fonction, pendant que vous mettez à jour le code.

N'utilisez pas d'API non publiques non documentées dans le code de votre fonction Lambda. Pour les AWS Lambda environnements d'exécution gérés, Lambda applique régulièrement des mises à jour fonctionnelles et de sécurité aux API internes de Lambda. Ces mises à jour internes de l'API peuvent être incompatibles avec les versions antérieures, entraînant des conséquences imprévues telles que des échecs d'invocation si votre fonction dépend de ces API non publiques. Consultez la Référence d'API pour obtenir la liste des API accessibles au public.

Écriture du code idempotent. L'écriture de code idempotent pour vos fonctions garantit ne gestion identique des événements dupliqués. Votre code doit valider correctement les événements et gérer correctement les événements dupliqués. Pour de plus amples informations, veuillez consulterComment faire en sorte que ma fonction Lambda soit idempotente ?.

Déployez les fonctions d'événement Ruby Lambda avec des archives de fichiers .zip

Le code de votre AWS Lambda fonction comprend un fichier .rb contenant le code du gestionnaire de votre fonction, ainsi que toutes les dépendances supplémentaires (gemmes) dont dépend votre code. Pour déployer ce code de fonction vers Lambda, vous utilisez un package de déploiement. Ce package peut être une archive de fichier .zip ou une image de conteneur. Pour plus d'informations sur l'utilisation d'images de conteneur avec Ruby, voir Déployer des fonctions d'événement Ruby Lambda avec des images de conteneur.

Pour créer votre package de déploiement sous forme d'archive de fichier .zip, vous pouvez utiliser l'utilitaire d'archivage .zip intégré à votre outil de ligne de commande, ou tout autre utilitaire .zip tel que 7zip. Les exemples présentés dans les sections suivantes supposent que vous utilisez un outil `zip` de ligne de commande dans un environnement Linux ou macOS. Pour utiliser les mêmes commandes sous Windows, vous pouvez installer le sous-système Windows pour Linux afin d'obtenir une Windows-integrated version d'Ubuntu et de Bash.

Notez que Lambda utilise les autorisations de fichiers POSIX. Ainsi, vous pourriez devoir définir des autorisations pour le dossier du package de déploiement avant de créer l'archive de fichiers .zip.

Les exemples de commandes présentés dans les sections suivantes utilisent l'utilitaire Bundler pour ajouter des dépendances à votre package de déploiement. Pour installer Bundler, exécutez la commande suivante.

```
gem install bundler
```

Sections

- Dépendances dans Ruby
- Création d'un package de déploiement .zip sans dépendances
- Création d'un package de déploiement .zip avec dépendances
- Création d'une couche Ruby pour vos dépendances
- Création de packages de déploiement .zip avec des bibliothèques natives
- Création et mise à jour des fonctions d'événement Ruby Lambda à l'aide de fichiers .zip

Dépendances dans Ruby

Pour les fonctions d'événement Lambda qui utilisent le runtime Ruby, une dépendance peut être n'importe quelle gemme Ruby. Lorsque vous déployez votre fonction à l'aide d'une archive .zip, vous

pouvez soit ajouter ces dépendances à votre fichier .zip avec votre code de fonction, soit utiliser une couche Lambda. Une couche est un fichier .zip séparé qui peut contenir du code supplémentaire et d'autres contenus. Pour en savoir plus sur l'utilisation des couches Lambda, consultez the section called "Layers".

L'environnement d'exécution Ruby inclut l' AWS SDK pour Ruby. Si votre fonction utilise le kit SDK, vous n'avez pas besoin de l'intégrer à votre code. Toutefois, pour garder le contrôle total de vos dépendances ou pour utiliser une version spécifique du kit SDK, vous pouvez l'ajouter au package de déploiement de votre fonction.

Vous pouvez inclure le kit SDK dans votre fichier .zip ou bien l'ajouter à l'aide d'une couche Lambda. Les dépendances de votre fichier .zip ou des couches Lambda sont prioritaires sur les versions incluses dans l'exécution. Pour savoir quelle version du kit SDK pour Ruby est incluse dans votre version d'exécution, consultez the section called "Runtime-included Versions du SDK".

Dans le cadre du modèle de responsabilité partagée AWS, vous êtes responsable de la gestion de toutes les dépendances dans les packages de déploiement de vos fonctions. Cela inclut l'application de mises à jour et de correctifs de sécurité. Pour mettre à jour les dépendances dans le package de déploiement de votre fonction, créez d'abord un nouveau fichier .zip, puis chargez-le sur Lambda. Pour plus d'informations, consultez Création d'un package de déploiement .zip avec dépendances et Création et mise à jour des fonctions d'événement Ruby Lambda à l'aide de fichiers .zip.

Création d'un package de déploiement .zip sans dépendances

Si le code de votre fonction ne comporte aucune dépendance, votre fichier .zip contient uniquement le fichier .rb contenant le code du gestionnaire de votre fonction. Utilisez votre utilitaire zip préféré pour créer un fichier .zip avec votre fichier .rb à la racine. Si le fichier .rb ne se trouve pas à la racine de votre fichier .zip, Lambda ne pourra pas exécuter votre code.

Pour savoir comment déployer votre fichier .zip pour créer une nouvelle fonction Lambda ou mettre à jour une fonction Lambda existante, veuillez consulter la rubrique Création et mise à jour des fonctions d'événement Ruby Lambda à l'aide de fichiers .zip.

Création d'un package de déploiement .zip avec dépendances

Si votre code de fonction dépend de GEM Ruby supplémentaires, vous pouvez soit ajouter ces dépendances à votre fichier .zip avec votre code de fonction, soit utiliser une couche Lambda. Les instructions de cette section vous indiquent comment inclure les dépendances dans votre package de déploiement .zip. Pour obtenir des instructions sur la façon d'inclure vos dépendances dans une couche, voir the section called "Création d'une couche Ruby pour vos dépendances".

Supposons que votre code de fonction soit enregistré dans un fichier nommé `lambda_function.rb` dans le répertoire de votre projet. L'exemple de commandes d'interface de ligne de commande suivant crée un fichier .zip nommé `my_deployment_package.zip` contenant le code de votre fonction et ses dépendances.

Pour créer le package de déploiement

1. Dans le répertoire de votre projet, créez un fichier `Gemfile` pour y spécifier vos dépendances.

   ```
   bundle init
   ```

2. En utilisant l'éditeur de texte de votre choix, modifiez le fichier `Gemfile` pour spécifier les dépendances de votre fonction. Par exemple, pour utiliser la GEM TZInfo, modifiez votre fichier `Gemfile` pour qu'il ressemble à ce qui suit.

   ```
   source "https://rubygems.org"
   gem "tzinfo"
   ```

3. Exécutez la commande suivante pour installer les GEM spécifiées dans votre fichier `Gemfile` dans votre répertoire de projet. Cette commande définit `vendor/bundle` comme chemin par défaut pour les installations de GEM.

   ```
   bundle config set --local path 'vendor/bundle' && bundle install
   ```

   Vous devez visualiser des résultats similaires à ce qui suit.

   ```
   Fetching gem metadata from https://rubygems.org/..........
   Resolving dependencies...
   Using bundler 2.4.13
   Fetching tzinfo 2.0.6
   Installing tzinfo 2.0.6
   ...
   ```

   > **Note**
   >
   > Pour réinstaller globalement les GEM ultérieurement, exécutez la commande suivante.
   >
   > ```
   > bundle config set --local system 'true'
   > ```

4. Créez une archive de fichiers .zip contenant le fichier `lambda_function.rb` avec le code du gestionnaire de votre fonction et les dépendances que vous avez installées à l'étape précédente.

```
zip -r my_deployment_package.zip lambda_function.rb vendor
```

Vous devez visualiser des résultats similaires à ce qui suit.

```
adding: lambda_function.rb (deflated 37%)
  adding: vendor/ (stored 0%)
  adding: vendor/bundle/ (stored 0%)
  adding: vendor/bundle/ruby/ (stored 0%)
  adding: vendor/bundle/ruby/3.2.0/ (stored 0%)
  adding: vendor/bundle/ruby/3.2.0/build_info/ (stored 0%)
  adding: vendor/bundle/ruby/3.2.0/cache/ (stored 0%)
  adding: vendor/bundle/ruby/3.2.0/cache/aws-eventstream-1.0.1.gem (deflated 36%)
...
```

Création d'une couche Ruby pour vos dépendances

Pour savoir comment empaqueter vos dépendances Ruby dans une couche Lambda, consultez the section called "Layers".

Création de packages de déploiement .zip avec des bibliothèques natives

De nombreuses gemmes Ruby courantes `nokogirinio4r`, telles que, et `mysql` contiennent des extensions natives écrites en C. Lorsque vous ajoutez des bibliothèques contenant du code C à votre package de déploiement, vous devez créer votre package correctement pour garantir sa compatibilité avec l'environnement d'exécution Lambda.

Pour les applications de production, nous vous recommandons de créer et de déployer votre code à l'aide de AWS Serverless Application Model (AWS SAM). AWS SAM Utilisez l'`sam build --use-container`option pour créer votre fonction dans un conteneur Lambda-like Docker. Pour en savoir plus sur l'utilisation AWS SAM de votre code de fonction pour déployer votre code de fonction, consultez la section Création d'applications dans le Guide du AWS SAM développeur.

Pour créer un package de déploiement .zip contenant des gemmes avec des extensions natives sans les utiliser AWS SAM, vous pouvez également utiliser un conteneur pour regrouper vos dépendances dans un environnement identique à l'environnement d'exécution Lambda Ruby. Pour réaliser ces

étapes, Docker doit être installé sur votre machine de génération. Pour en savoir plus sur l'installation de Docker, consultez Installation du moteur Docker.

Pour créer un package de déploiement .zip dans un conteneur Docker

1. Créez un dossier sur votre machine de génération locale pour y enregistrer votre conteneur. Dans ce dossier, créez un fichier nommé `dockerfile` et collez-y le code suivant.

   ```
   FROM public.ecr.aws/sam/build-ruby3.2:latest-x86_64
   RUN gem update bundler
   CMD "/bin/bash"
   ```

2. Dans le dossier dans lequel vous avez créé votre fichier `dockerfile`, exécutez la commande suivante pour créer le conteneur Docker.

   ```
   docker build -t awsruby32 .
   ```

3. Accédez au répertoire du projet contenant le fichier `.rb` avec le code du gestionnaire de votre fonction et le fichier `Gemfile` spécifiant les dépendances de votre fonction. À partir de ce répertoire, exécutez la commande suivante pour démarrer le conteneur Lambda Ruby.

   Linux/MacOS

   ```
   docker run --rm -it -v $PWD:/var/task -w /var/task awsruby32
   ```

   > **Note**
   >
   > Sous macOS, il se peut qu'un avertissement vous informe que la plateforme de l'image demandée ne correspond pas à la plateforme de l'hôte détectée. Ignorez cet avertissement.

   Windows PowerShell

   ```
   docker run --rm -it -v ${pwd}:/var/task -w /var/task awsruby32
   ```

   Lorsque votre conteneur démarre, vous devriez voir une invite bash.

```
bash-4.2#
```

4. Configurez l'utilitaire bundle pour installer les GEM spécifiées dans votre fichier `Gemfile` dans votre répertoire `vendor/bundle` local et installer vos dépendances.

```
bash-4.2# bundle config set --local path 'vendor/bundle' && bundle install
```

5. Créez le package de déploiement .zip avec le code de votre fonction et ses dépendances. Dans cet exemple, le fichier contenant le code du gestionnaire de votre fonction est nommé `lambda_function.rb`.

```
bash-4.2# zip -r my_deployment_package.zip lambda_function.rb vendor
```

6. Quittez le conteneur et retournez dans votre répertoire de projet local.

```
bash-4.2# exit
```

   Vous pouvez désormais utiliser le package de déploiement du fichier .zip pour créer ou mettre à jour votre fonction Lambda. Consultez Création et mise à jour des fonctions d'événement Ruby Lambda à l'aide de fichiers .zip

Création et mise à jour des fonctions d'événement Ruby Lambda à l'aide de fichiers .zip

Une fois que vous avez créé votre package de déploiement .zip, vous pouvez l'utiliser pour créer une nouvelle fonction Lambda ou mettre à jour une fonction Lambda existante. Vous pouvez déployer votre package .zip à l'aide de la console Lambda, de l'API Lambda et AWS Command Line Interface de l'API Lambda. Vous pouvez également créer et mettre à jour des fonctions Lambda à l'aide de l' AWS Serverless Application Model (AWS SAM) et de CloudFormation.

La taille maximale d'un package de déploiement .zip pour Lambda est de 250 Mo (décompressé). Notez que cette limite s'applique à la taille combinée de tous les fichiers que vous chargez, y compris les couches Lambda.

Le runtime Lambda a besoin d'une autorisation pour lire les fichiers de votre package de déploiement. Dans la notation octale des autorisations Linux, Lambda a besoin de 644 autorisations pour les fichiers non exécutables (rw-r--r--) et de 755 autorisations (rwxr-xr-x) pour les répertoires et les fichiers exécutables.

Sous Linux et macOS, utilisez la commande chmod pour modifier les autorisations de fichiers sur les fichiers et les répertoires de votre package de déploiement. Par exemple, pour octroyer à un fichier non exécutable les autorisations correctes, exécutez la commande suivante.

```
chmod 644 <filepath>
```

Pour modifier les autorisations relatives aux fichiers dans Windows, voir Définir, afficher, modifier ou supprimer des autorisations sur un objet dans la documentation Microsoft Windows.

> **Note**
>
> Si vous n'octroyez pas à Lambda les autorisations dont il a besoin pour accéder aux répertoires de votre package de déploiement, Lambda définit les autorisations de ces répertoires à 755 (rwxr-xr-x).

Création et mise à jour de fonctions avec des fichiers .zip à l'aide de la console

Pour créer une nouvelle fonction, vous devez d'abord créer la fonction dans la console, puis charger votre archive .zip. Pour mettre à jour une fonction existante, ouvrez la page de votre fonction, puis suivez la même procédure pour ajouter votre fichier .zip mis à jour.

Si votre fichier .zip fait moins de 50 Mo, vous pouvez créer ou mettre à jour une fonction en chargeant le fichier directement à partir de votre ordinateur local. Pour les fichiers .zip de plus de 50 Mo, vous devez d'abord charger votre package dans un compartiment Amazon S3. Pour savoir comment charger un fichier dans un compartiment Amazon S3 à l'aide du Console de gestion AWS, consultez Getting started with Amazon S3. Pour télécharger des fichiers à l'aide de AWS CLI, voir Déplacer des objets dans le guide de AWS CLI l'utilisateur.

> **Note**
>
> Vous ne pouvez pas modifier le type de package de déploiement (.zip ou image de conteneur) d'une fonction existante. Par exemple, vous ne pouvez pas convertir une fonction d'image de conteneur pour utiliser un fichier d'archive .zip à la place. Vous devez créer une nouvelle fonction.

Pour créer une nouvelle fonction (console)

1. Ouvrez la page Event Functions de la console Lambda et choisissez Create Event Function.
2. Choisissez Créer à partir de zéro.
3. Sous Informations de base, procédez comme suit :
    a. Pour Nom de la fonction, saisissez le nom de la fonction.
    b. Pour Exécution, sélectionnez l'exécution que vous souhaitez utiliser.
    c. (Facultatif) Pour Architecture, choisissez l'architecture de l'ensemble des instructions pour votre fonction. L'architecture par défaut est x86_64. Assurez-vous que le package de déploiement .zip pour votre fonction est compatible avec l'architecture de l'ensemble d'instructions que vous sélectionnez.
4. (Facultatif) Sous Permissions (Autorisations), développez Change default execution role (Modifier le rôle d'exécution par défaut). Vous pouvez créer un rôle d'exécution ou en utiliser un existant.
5. Choisissez Create Event Function. Lambda crée une fonction de base « Hello world » à l'aide de l'exécution de votre choix.

Pour charger une archive .zip à partir de votre ordinateur local (console)

1. Sur la page Event Functions de la console Lambda, choisissez la fonction pour laquelle vous souhaitez télécharger le fichier .zip.
2. Sélectionnez l'onglet Code.
3. Dans le volet Source du code, choisissez Charger à partir de.
4. Choisissez Fichier .zip.
5. Pour charger un fichier .zip, procédez comme suit :
    a. Sélectionnez Charger, puis choisissez votre fichier .zip dans le sélecteur de fichiers.
    b. Choisissez Ouvrir.
    c. Cliquez sur Enregistrer.

Pour charger une archive .zip depuis un compartiment Amazon S3 (console)

1. Sur la page Event Functions de la console Lambda, choisissez la fonction pour laquelle vous souhaitez télécharger un nouveau fichier .zip.

2. Sélectionnez l'onglet Code.
3. Dans le volet Source du code, choisissez Charger à partir de.
4. Choisissez l'emplacement Amazon S3.
5. Collez l'URL du lien Amazon S3 de votre fichier .zip et choisissez Enregistrer.

Mise à jour des fonctions du fichier .zip à l'aide de l'éditeur de code de la console

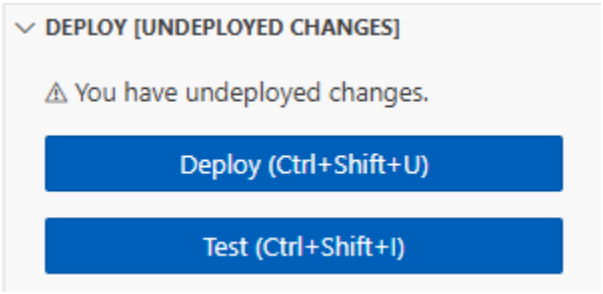
Pour certaines fonctions avec des packages de déploiement .zip, vous pouvez utiliser l'éditeur de code intégré de la console Lambda pour mettre à jour le code de votre fonction directement. Pour utiliser cette fonctionnalité, votre fonction doit répondre aux critères suivants :

- Votre fonction doit utiliser l'un des environnements d'exécution du langage interprété (Python ou Ruby) Node.js
- La taille du package de déploiement de votre fonction doit être inférieure à 50 Mo (décompressé).

Le code des fonctions avec les packages de déploiement d'images de conteneurs ne peut pas être édité directement dans la console.

Pour mettre à jour le code de fonction à l'aide de l'éditeur de code de la console

1. Ouvrez la page Event Functions de la console Lambda et sélectionnez votre fonction.
2. Sélectionnez l'onglet Code.
3. Dans le volet Source du code, sélectionnez votre fichier de code source et modifiez-le dans l'éditeur de code intégré.
4. Dans la section DÉPLOYER, choisissez Déployer pour mettre à jour le code de votre fonction :



Création et mise à jour de fonctions avec des fichiers .zip à l'aide du AWS CLI

Vous pouvez utiliser l'AWS CLI pour créer une nouvelle fonction ou pour mettre à jour une fonction existante à l'aide d'un fichier .zip. Utilisez les commandes create-function et update-function-code

pour déployer votre package .zip. Si votre fichier .zip est inférieur à 50 Mo, vous pouvez charger le package .zip à partir d'un emplacement de fichier sur votre machine de génération locale. Pour les fichiers plus volumineux, vous devez charger votre package .zip à partir d'un compartiment Amazon S3. Pour savoir comment charger un fichier dans un compartiment Amazon S3 à l'aide du AWS CLI, consultez la section Déplacer des objets dans le guide de AWS CLI l'utilisateur.

> **Note**
>
> Si vous chargez votre fichier .zip depuis un compartiment Amazon S3 à l'aide de AWS CLI, le compartiment doit se trouver au même endroit Région AWS que votre fonction.

Pour créer une nouvelle fonction à l'aide d'un fichier .zip avec le AWS CLI, vous devez spécifier les éléments suivants :

- Le nom de votre fonction (`--function-name`)
- L'exécution de votre fonction (`--runtime`)
- L'Amazon Resource Name (ARN) du rôle d'exécution de votre fonction (`--role`)
- Le nom de la méthode du gestionnaire dans votre code de fonction (`--handler`)

Vous devez également indiquer l'emplacement de votre fichier .zip. Si votre fichier .zip se trouve dans un dossier sur votre machine de génération locale, utilisez l'option `--zip-file` pour spécifier le chemin d'accès du fichier, comme le montre l'exemple de commande suivant.

```
aws lambda create-function --function-name myFunction \
--runtime ruby3.2 --handler lambda_function.lambda_handler \
--role arn:aws:iam::111122223333:role/service-role/my-lambda-role \
--zip-file fileb://myFunction.zip
```

Pour spécifier l'emplacement du fichier .zip dans un compartiment Amazon S3, utilisez l'option `--code` comme le montre l'exemple de commande suivant. Vous devez uniquement utiliser le paramètre `S3ObjectVersion` pour les objets soumis à la gestion des versions.

```
aws lambda create-function --function-name myFunction \
--runtime ruby3.2 --handler lambda_function.lambda_handler \
--role arn:aws:iam::111122223333:role/service-role/my-lambda-role \
--code S3Bucket=amzn-s3-demo-
bucket,S3Key=myFileName.zip,S3ObjectVersion=myObjectVersion
```

Pour mettre à jour une fonction existante à l'aide de l'interface de ligne de commande, vous devez spécifier le nom de votre fonction à l'aide du paramètre `--function-name`. Vous devez également spécifier l'emplacement du fichier .zip que vous souhaitez utiliser pour mettre à jour votre code de fonction. Si votre fichier .zip se trouve dans un dossier sur votre machine de génération locale, utilisez l'option `--zip-file` pour spécifier le chemin d'accès du fichier, comme le montre l'exemple de commande suivant.

```
aws lambda update-function-code --function-name myFunction \
--zip-file fileb://myFunction.zip
```

Pour spécifier l'emplacement du fichier .zip dans un compartiment Amazon S3, utilisez les options `--s3-bucket` et `--s3-key` comme le montre l'exemple de commande suivant. Vous devez uniquement utiliser le paramètre `--s3-object-version` pour les objets soumis à la gestion des versions.

```
aws lambda update-function-code --function-name myFunction \
--s3-bucket amzn-s3-demo-bucket --s3-key myFileName.zip --s3-object-version myObject
 Version
```

Création et mise à jour de fonctions avec des fichiers .zip à l'aide de l'API Lambda

Pour créer et mettre à jour des fonctions à l'aide d'une archive de fichiers .zip, utilisez les opérations d'API suivantes :

- CreateFunction
- UpdateFunctionCode

Création et mise à jour de fonctions avec des fichiers .zip à l'aide de AWS SAM

The AWS Serverless Application Model (AWS SAM) est une boîte à outils qui permet de rationaliser le processus de création et d'exécution d'applications sans serveur sur AWS. Vous définissez les ressources de votre application dans un modèle YAML ou JSON et vous utilisez l'interface de ligne de AWS SAM commande (AWS SAM CLI) pour créer, empaqueter et déployer vos applications. Lorsque vous créez une fonction Lambda à partir d'un AWS SAM modèle, elle crée AWS SAM automatiquement un package de déploiement ou une image de conteneur .zip avec le code de votre fonction et les dépendances que vous spécifiez. Pour en savoir plus sur l'utilisation des fonctions Lambda AWS SAM pour créer et déployer des fonctions Lambda, consultez Getting started with AWS SAM dans le Guide du AWS Serverless Application Model développeur.

Vous pouvez également l'utiliser AWS SAM pour créer une fonction Lambda à l'aide d'une archive de fichiers .zip existante. Pour créer une fonction Lambda à l'aide de AWS SAM, vous pouvez enregistrer votre fichier .zip dans un compartiment Amazon S3 ou dans un dossier local sur votre machine de génération. Pour savoir comment charger un fichier dans un compartiment Amazon S3 à l'aide du AWS CLI, consultez la section Déplacer des objets dans le guide de AWS CLI l'utilisateur.

Dans votre AWS SAM modèle, la `AWS::Serverless::Function` ressource spécifie votre fonction Lambda. Dans cette ressource, définissez les propriétés suivantes pour créer une fonction à l'aide d'une archive de fichiers .zip :

- `PackageType` : défini sur `Zip`
- `CodeUri`- défini sur l'URI Amazon S3, le chemin d'accès au dossier local ou à l'FunctionCodeobjet du code de fonction
- `Runtime` : défini sur votre exécution choisie

Ainsi AWS SAM, si votre fichier .zip est supérieur à 50 Mo, vous n'avez pas besoin de le télécharger au préalable dans un compartiment Amazon S3. AWS SAM peut télécharger des packages .zip jusqu'à la taille maximale autorisée de 250 Mo (décompressés) à partir d'un emplacement sur votre machine de compilation locale.

Pour en savoir plus sur le déploiement de fonctions à l'aide d'un fichier .zip dans AWS SAM, voir AWS::Serverless::Function dans le manuel du AWS SAM développeur.

Création et mise à jour de fonctions avec des fichiers .zip à l'aide de CloudFormation

Vous pouvez l'utiliser CloudFormation pour créer une fonction Lambda à l'aide d'une archive de fichiers .zip. Pour créer une fonction Lambda à partir d'un fichier .zip, vous devez d'abord charger votre fichier dans un compartiment Amazon S3. Pour savoir comment charger un fichier dans un compartiment Amazon S3 à l'aide du AWS CLI, consultez la section Déplacer des objets dans le guide de AWS CLI l'utilisateur.

Dans votre CloudFormation modèle, la `AWS::Lambda::Function` ressource spécifie votre fonction Lambda. Dans cette ressource, définissez les propriétés suivantes pour créer une fonction à l'aide d'une archive de fichiers .zip :

- `PackageType` : défini sur `Zip`
- `Code` : saisissez le nom du compartiment Amazon S3 et le nom du fichier .zip dans les champs `S3Bucket` et `S3Key`
- `Runtime` : défini sur votre exécution choisie

Le fichier .zip CloudFormation généré ne peut pas dépasser 4 Mo. Pour en savoir plus sur le déploiement de fonctions à l'aide d'un fichier .zip dans CloudFormation, voir AWS::Lambda::Function dans le guide de l'CloudFormation utilisateur.

Déployez les fonctions d'événement Ruby Lambda avec des images de conteneur

Il existe trois méthodes pour créer une image de conteneur pour une fonction d'événement Ruby Lambda :

- À l'aide d'un AWS image de base pour Ruby

  Les images de base AWS sont préchargées avec une exécution du langage, un client d'interface d'exécution pour gérer l'interaction entre Lambda et votre code de fonction, et un émulateur d'interface d'exécution pour les tests locaux.
- À l'aide d'un AWS OS-only image de base

  AWS OS-only les images de base contiennent une distribution Amazon Linux et l'émulateur d'interface d'exécution. Ces images sont couramment utilisées pour créer des images de conteneur pour les langages compilés, tels que Go et Rust, et pour une langue ou une version linguistique pour laquelle Lambda ne fournit pas d'image de base, telle que Node.js 19. Vous pouvez également utiliser des images OS-only de base pour implémenter un environnement d'exécution personnalisé. Pour rendre l'image compatible avec Lambda, vous devez inclure le client d'interface d'exécution pour Ruby dans l'image.
- Utilisation d'une image non AWS basique

  Vous pouvez utiliser une autre image de base à partir d'un autre registre de conteneur, comme Alpine Linux ou Debian. Vous pouvez également utiliser une image personnalisée créée par votre organisation. Pour rendre l'image compatible avec Lambda, vous devez inclure le client d'interface d'exécution pour Ruby dans l'image.

> **Tip**
>
> Pour réduire le temps nécessaire à l'activation des fonctions du conteneur Lambda, consultez Utiliser des générations en plusieurs étapes (français non garanti) dans la documentation Docker. Pour créer des images de conteneur efficaces, suivez la section Bonnes pratiques pour l'écriture de Dockerfiles (français non garanti).

Cette page explique comment créer, tester et déployer des images de conteneur pour Lambda.

Rubriques

- AWS images de base pour Ruby

- À l'aide d'un AWS image de base pour Ruby
- Utilisation d’une autre image de base avec le client d’interface d’exécution

AWS images de base pour Ruby

AWS fournit les images de base suivantes pour Ruby :

Étiquettes	Environnement d’exécution	Système d’exploitation	Dockerfile	Obsolescence
4.0	Ruby 4.0	Amazon Linux	Dockerfile pour Ruby 4.0 sur GitHub	31 mars 2029
3.4	Ruby 3.4	Amazon Linux	Dockerfile pour Ruby 3.4 sur GitHub	31 mars 2028
3.3	Ruby 3.3	Amazon Linux	Dockerfile pour Ruby 3.3 sur GitHub	31 mars 2027

Référentiel Amazon ECR : gallery.ecr. aws/lambda/rubis

À l'aide d'un AWS image de base pour Ruby

Conditions préalables

Pour exécuter la procédure indiquée dans cette section, vous devez satisfaire aux exigences suivantes :

- AWS CLI version 2
- Docker (version minimale 25.0.0)
- Le plug-in buildx Docker.
- Ruby

Création d'une image à partir d'une image de base

Pour créer une image de conteneur pour Ruby

1. Créez un répertoire pour le projet, puis passez à ce répertoire.

```
mkdir example
cd example
```

2. Créez un nouveau fichier appelé `Gemfile`. C'est ici que vous listez les RubyGems packages requis pour votre application. Le AWS SDK pour Ruby est disponible auprès de RubyGems. Vous devez choisir des gemmes AWS de service spécifiques à installer. Par exemple, pour utiliser la gem Ruby pour Lambda, votre Gemfile doit ressembler à ceci :

```
source 'https://rubygems.org'

gem 'aws-sdk-lambda'
```

   Sinon, la gemme aws-sdk contient toutes les gemmes de service disponibles. AWS Cette gem est très large. Nous vous recommandons de ne l'utiliser que si vous dépendez de nombreux AWS services.

3. Installez les dépendances spécifiées dans le fichier Gemfile à l'aide de l'installation groupée.

```
bundle install
```

4. Créez un nouveau fichier appelé `lambda_function.rb`. Vous pouvez ajouter l'exemple de code de fonction suivant au fichier pour le tester, ou utiliser le vôtre.

   Example Fonction Ruby

```
module LambdaFunction
  class Handler
    def self.process(event:,context:)
      "Hello from Lambda!"
    end
  end
end
```

5. Créez un nouveau fichier Docker. Voici un exemple de Dockerfile qui utilise une image de base AWS. Le Dockerfile utilise la configuration suivante :

- Définissez la propriété FROM sur l'URI de l'image de base.
- Utilisez la commande COPY pour copier le code de fonction et les dépendances d'{LAMBDA_TASK_ROOT}exécution dans une variable d'Lambda-defined environnement.
- Définir l'argument CMD pour le gestionnaire de la fonction Lambda.

Notez que l'exemple de Dockerfile n'inclut pas d'instruction USER. Lorsque vous déployez une image de conteneur sur Lambda, Lambda définit automatiquement un utilisateur Linux par défaut disposant d'autorisations de moindre privilège. Ceci est différent du comportement standard de Docker qui est défini par défaut par l'utilisateur `root` lorsqu'aucune instruction USER n'est fournie.

Example Dockerfile

```
FROM public.ecr.aws/lambda/ruby:3.4

# Copy Gemfile and Gemfile.lock
COPY Gemfile Gemfile.lock ${LAMBDA_TASK_ROOT}/

# Install Bundler and the specified gems
RUN gem install bundler:2.4.20 && \
    bundle config set --local path 'vendor/bundle' && \
    bundle install

# Copy function code
COPY lambda_function.rb ${LAMBDA_TASK_ROOT}/

# Set the CMD to your handler (could also be done as a parameter override outside
 of the Dockerfile)
CMD [ "lambda_function.LambdaFunction::Handler.process" ]
```

6. Générez l'image Docker à l'aide de la commande docker build. L'exemple suivant nomme l'image `docker-image` et lui donne la balise `test`. Pour rendre votre image compatible avec Lambda, vous devez utiliser l'option `--provenance=false`.

```
docker buildx build --platform linux/amd64 --provenance=false -t docker-image:test
 .
```

> **Note**
>
> La commande spécifie l'option `--platform linux/amd64` pour garantir la compatibilité de votre conteneur avec l'environnement d'exécution Lambda, quelle que soit l'architecture de votre machine de génération. Si vous avez l'intention de créer une fonction Lambda à l'aide de l'architecture du jeu d'instructions ARM64, veillez à modifier la commande pour utiliser plutôt l'option `--platform linux/arm64`.

(Facultatif) Testez l'image localement

1. Démarrez votre image Docker à l'aide de la commande docker run. Dans cet exemple, `docker-image` est le nom de l'image et `test` est la balise.

   ```
   docker run --platform linux/amd64 -p 9000:8080 docker-image:test
   ```

   Cette commande exécute l'image en tant que conteneur et crée un point de terminaison local à `localhost:9000/2015-03-31/functions/function/invocations`.

   > **Note**
   >
   > Si vous avez créé l'image Docker pour l'architecture du jeu d'instructions ARM64, veillez à utiliser l'option `--platform linux/arm64` plutôt que `--platform linux/amd64`.

2. À partir d'une nouvelle fenêtre de terminal, publiez un événement au point de terminaison local.

   Linux/macOS

   Sous Linux et macOS, exécutez la commande `curl` suivante :

   ```
   curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d '{}'
   ```

   Cette commande invoque la fonction avec un événement vide et renvoie une réponse. Si vous utilisez votre propre code de fonction plutôt que l'exemple de code de fonction, vous pouvez invoquer la fonction avec une charge utile JSON. Exemple :

```
curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d
 '{"payload":"hello world!"}'
```

PowerShell

Dans PowerShell, exécutez la `Invoke-WebRequest` commande suivante :

```
Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/
invocations" -Method Post -Body '{}' -ContentType "application/json"
```

Cette commande invoque la fonction avec un événement vide et renvoie une réponse. Si vous utilisez votre propre code de fonction plutôt que l'exemple de code de fonction, vous pouvez invoquer la fonction avec une charge utile JSON. Exemple :

```
Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/
invocations" -Method Post -Body '{"payload":"hello world!"}' -ContentType
 "application/json"
```

3. Obtenez l'ID du conteneur.

```
docker ps
```

4. Utilisez la commande docker kill pour arrêter le conteneur. Dans cette commande, remplacez `3766c4ab331c` par l'ID du conteneur de l'étape précédente.

```
docker kill 3766c4ab331c
```

Déploiement de l'image

Pour charger l'image sur Amazon RIE et créer la fonction Lambda

1. Exécutez la commande get-login-password pour authentifier la CLI Docker auprès de votre registre Amazon ECR.
   - Définissez la `--region` valeur à l' Région AWS endroit où vous souhaitez créer le référentiel Amazon ECR.
   - `111122223333`Remplacez-le par votre Compte AWS identifiant.

```
aws ecr get-login-password --region us-east-1 | docker login --username AWS --
password-stdin 111122223333.dkr.ecr.us-east-1.amazonaws.com
```

2. Créez un référentiel dans Amazon ECR à l'aide de la commande create-repository.

```
aws ecr create-repository --repository-name hello-world --region us-east-1 --image-
scanning-configuration scanOnPush=true --image-tag-mutability MUTABLE
```

> **Note**
>
> Le référentiel Amazon ECR doit être Région AWS identique à la fonction Lambda.

En cas de succès, vous obtenez une réponse comme celle-ci :

```
{
    "repository": {
        "repositoryArn": "arn:aws:ecr:us-east-1:111122223333:repository/hello-
world",
        "registryId": "111122223333",
        "repositoryName": "hello-world",
        "repositoryUri": "111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-
world",
        "createdAt": "2023-03-09T10:39:01+00:00",
        "imageTagMutability": "MUTABLE",
        "imageScanningConfiguration": {
            "scanOnPush": true
        },
        "encryptionConfiguration": {
            "encryptionType": "AES256"
        }
    }
}
```

3. Copiez le `repositoryUri` à partir de la sortie de l'étape précédente.
4. Exécutez la commande docker tag pour étiqueter votre image locale dans votre référentiel Amazon ECR en tant que dernière version. Dans cette commande :

- `docker-image:test` est le nom et la balise de votre image Docker. Il s'agit du nom et de la balise de l'image que vous avez spécifiés dans la commande `docker build`.
- Remplacez `<ECRrepositoryUri>` par l'`repositoryUri` que vous avez copié. Assurez-vous d'inclure `:latest` à la fin de l'URI.

```
docker tag docker-image:test <ECRrepositoryUri>:latest
```

Exemple :

```
docker tag docker-image:test 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

5. Exécutez la commande docker push pour déployer votre image locale dans le référentiel Amazon ECR. Assurez-vous d'inclure `:latest` à la fin de l'URI du référentiel.

```
docker push 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

6. Créez un rôle d'exécution pour la fonction, si vous n'en avez pas déjà un. Vous aurez besoin de l'Amazon Resource Name (ARN) du rôle à l'étape suivante.
7. Créez la fonction Lambda. Pour `ImageUri`, indiquez l'URI du référentiel mentionné précédemment. Assurez-vous d'inclure `:latest` à la fin de l'URI.

```
aws lambda create-function \
  --function-name hello-world \
  --package-type Image \
  --code ImageUri=111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \
  --role arn:aws:iam::111122223333:role/lambda-ex
```

> **Note**
>
> Vous pouvez créer une fonction en utilisant une image d'un autre AWS compte, à condition que l'image se trouve dans la même région que la fonction Lambda. Pour plus d'informations, consultez Autorisations entre comptes Amazon ECR.

8. Invoquer la fonction.

```
aws lambda invoke --function-name hello-world response.json
```

Vous devriez obtenir une réponse comme celle-ci :

```
{
  "ExecutedVersion": "$LATEST",
  "StatusCode": 200
}
```

9. Pour voir la sortie de la fonction, consultez le fichier `response.json`.

Pour mettre à jour le code de la fonction, vous devez recréer l'image, charger la nouvelle image dans le référentiel Amazon ECR, puis utiliser la commande update-function-code pour déployer l'image dans la fonction Lambda.

Lambda résout l'étiquette d'image en hachage d'image spécifique. Cela signifie que si vous pointez la balise d'image qui a été utilisée pour déployer la fonction vers une nouvelle image dans Amazon ECR, Lambda ne met pas automatiquement à jour la fonction pour utiliser la nouvelle image.

Pour déployer la nouvelle image sur la même fonction Lambda, vous devez utiliser la commande update-function-code, même si la balise d'image dans Amazon ECR reste la même. Dans l'exemple suivant, l'option `--publish` crée une version de la fonction à l'aide de l'image du conteneur mise à jour.

```
aws lambda update-function-code \
  --function-name hello-world \
  --image-uri 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \
  --publish
```

Utilisation d'une autre image de base avec le client d'interface d'exécution

Si vous utilisez une image OS-only de base ou une image de base alternative, vous devez inclure le client d'interface d'exécution dans votre image. Le client d'interface d'exécution étend leAPI de runtime, qui gère l'interaction entre Lambda et votre code de fonction.

Installez le client d'interface d'exécution Lambda pour Ruby à l'aide du gestionnaire de RubyGems.org packages :

```
gem install aws_lambda_ric
```

Vous pouvez également télécharger le client d'interface d'exécution Ruby depuis GitHub.

L'exemple suivant montre comment créer une image de conteneur pour Ruby à l'aide d'une image non AWS basique. L'exemple Dockerfile utilise une image de base Ruby officielle. Le Dockerfile inclut le client d'interface d'exécution.

Conditions préalables

Pour exécuter la procédure indiquée dans cette section, vous devez satisfaire aux exigences suivantes :

- AWS CLI version 2
- Docker (version minimale 25.0.0)
- Le plug-in buildx Docker.
- Ruby

Création d'une image à partir d'une image de base alternative

Pour créer une image de conteneur pour Ruby au moyen d'une autre image de base

1. Créez un répertoire pour le projet, puis passez à ce répertoire.

```
mkdir example
cd example
```

2. Créez un nouveau fichier appelé `Gemfile`. C'est ici que vous listez les RubyGems packages requis pour votre application. Le AWS SDK pour Ruby est disponible auprès de RubyGems. Vous devez choisir des gemmes AWS de service spécifiques à installer. Par exemple, pour utiliser la gem Ruby pour Lambda, votre Gemfile doit ressembler à ceci :

```
source 'https://rubygems.org'

gem 'aws-sdk-lambda'
```

   Sinon, la gemme aws-sdk contient toutes les gemmes de service disponibles. AWS Cette gem est très large. Nous vous recommandons de ne l'utiliser que si vous dépendez de nombreux AWS services.

3. Installez les dépendances spécifiées dans le fichier Gemfile à l'aide de l'installation groupée.

```
bundle install
```

4. Créez un nouveau fichier appelé `lambda_function.rb`. Vous pouvez ajouter l'exemple de code de fonction suivant au fichier pour le tester, ou utiliser le vôtre.

   Example Fonction Ruby

   ```
   module LambdaFunction
     class Handler
       def self.process(event:,context:)
         "Hello from Lambda!"
       end
     end
   end
   ```

5. Créez un nouveau fichier Docker. Le Dockerfile suivant utilise une image de base Ruby au lieu d'une image de base AWS. Le Dockerfile inclut le client d'interface d'exécution pour Ruby, ce qui rend l'image compatible avec Lambda. Vous pouvez également ajouter le client de l'interface d'exécution au Gemfile de votre application.

   - Définissez la propriété `FROM` sur l'image de base Ruby.
   - Créez un répertoire pour le code de fonction et une variable d'environnement pointant vers ce répertoire. Dans cet exemple, le répertoire est `/var/task`, qui reflète l'environnement d'exécution Lambda. Cependant, vous pouvez choisir n'importe quel répertoire pour le code de fonction car le Dockerfile n'utilise pas d'image de AWS base.
   - Définissez le `ENTRYPOINT` sur le module que vous souhaitez que le conteneur Docker exécute lorsqu'il démarre. Dans ce cas, le module est le client d'interface d'exécution.
   - Définir l'argument `CMD` pour le gestionnaire de la fonction Lambda.

   Notez que l'exemple de Dockerfile n'inclut pas d'instruction USER. Lorsque vous déployez une image de conteneur sur Lambda, Lambda définit automatiquement un utilisateur Linux par défaut disposant d'autorisations de moindre privilège. Ceci est différent du comportement standard de Docker qui est défini par défaut par l'utilisateur `root` lorsqu'aucune instruction `USER` n'est fournie.

   Example Dockerfile

   ```
   FROM ruby:2.7
   ```

```
# Install the runtime interface client for Ruby
RUN gem install aws_lambda_ric

# Add the runtime interface client to the PATH
ENV PATH="/usr/local/bundle/bin:${PATH}"

# Create a directory for the Lambda function
ENV LAMBDA_TASK_ROOT=/var/task
RUN mkdir -p ${LAMBDA_TASK_ROOT}
WORKDIR ${LAMBDA_TASK_ROOT}

# Copy Gemfile and Gemfile.lock
COPY Gemfile Gemfile.lock ${LAMBDA_TASK_ROOT}/

# Install Bundler and the specified gems
RUN gem install bundler:2.4.20 && \
    bundle config set --local path 'vendor/bundle' && \
    bundle install

# Copy function code
COPY lambda_function.rb ${LAMBDA_TASK_ROOT}/

# Set runtime interface client as default command for the container runtime
ENTRYPOINT [ "aws_lambda_ric" ]

# Set the CMD to your handler (could also be done as a parameter override outside
 of the Dockerfile)
CMD [ "lambda_function.LambdaFunction::Handler.process" ]
```

6. Générez l'image Docker à l'aide de la commande docker build. L'exemple suivant nomme l'image `docker-image` et lui donne la balise `test`. Pour rendre votre image compatible avec Lambda, vous devez utiliser l'option `--provenance=false`.

```
docker buildx build --platform linux/amd64 --provenance=false -t docker-image:test
 .
```

> **Note**
>
> La commande spécifie l'option `--platform linux/amd64` pour garantir la compatibilité de votre conteneur avec l'environnement d'exécution Lambda, quelle que soit l'architecture de votre machine de génération. Si vous avez l'intention de créer une

fonction Lambda à l'aide de l'architecture du jeu d'instructions ARM64, veillez à modifier la commande pour utiliser plutôt l'option `--platform linux/arm64`.

(Facultatif) Testez l'image localement

Utilisez l'émulateur d'interface d'exécution pour tester l'image localement. Vous pouvez intégrer l'émulateur dans votre image ou utiliser la procédure suivante pour l'installer sur votre machine locale.

Pour installer et exécuter l'émulateur d'interface d'exécution sur votre ordinateur local

1. Depuis le répertoire de votre projet, exécutez la commande suivante pour télécharger l'émulateur d'interface d'exécution (architecture x86-64) GitHub et l'installer sur votre machine locale.

   Linux/macOS

   ```
   mkdir -p ~/.aws-lambda-rie && \
       curl -Lo ~/.aws-lambda-rie/aws-lambda-rie https://github.com/aws/aws-lambda-runtime-interface-emulator/releases/latest/download/aws-lambda-rie && \
       chmod +x ~/.aws-lambda-rie/aws-lambda-rie
   ```

   Pour installer l'émulateur arm64, remplacez l'URL du GitHub référentiel dans la commande précédente par la suivante :

   ```
   https://github.com/aws/aws-lambda-runtime-interface-emulator/releases/latest/download/aws-lambda-rie-arm64
   ```

   PowerShell

   ```
   $dirPath = "$HOME\.aws-lambda-rie"
   if (-not (Test-Path $dirPath)) {
       New-Item -Path $dirPath -ItemType Directory
   }

   $downloadLink = "https://github.com/aws/aws-lambda-runtime-interface-emulator/releases/latest/download/aws-lambda-rie"
   $destinationPath = "$HOME\.aws-lambda-rie\aws-lambda-rie"
   Invoke-WebRequest -Uri $downloadLink -OutFile $destinationPath
   ```

Pour installer l'émulateur arm64, remplacez `$downloadLink` par ce qui suit :

```
https://github.com/aws/aws-lambda-runtime-interface-emulator/releases/latest/
download/aws-lambda-rie-arm64
```

2. Démarrez votre image Docker à l'aide de la commande docker run. Notez ce qui suit :

   - `docker-image` est le nom de l'image et `test` est la balise.
   - `aws_lambda_ric lambda_function.LambdaFunction::Handler.process` est le ENTRYPOINT suivi du CMD depuis votre Dockerfile.

   Linux/macOS

   ```
   docker run --platform linux/amd64 -d -v ~/.aws-lambda-rie:/aws-lambda -p
    9000:8080 \
       --entrypoint /aws-lambda/aws-lambda-rie \
       docker-image:test \
           aws_lambda_ric lambda_function.LambdaFunction::Handler.process
   ```

   PowerShell

   ```
   docker run --platform linux/amd64 -d -v "$HOME\.aws-lambda-rie:/aws-lambda" -p
    9000:8080 `
   --entrypoint /aws-lambda/aws-lambda-rie `
   docker-image:test `
       aws_lambda_ric lambda_function.LambdaFunction::Handler.process
   ```

   Cette commande exécute l'image en tant que conteneur et crée un point de terminaison local à `localhost:9000/2015-03-31/functions/function/invocations`.

   > **Note**
   >
   > Si vous avez créé l'image Docker pour l'architecture du jeu d'instructions ARM64, veillez à utiliser l'option `--platform linux/arm64` plutôt que `--platform linux/amd64`.

3. Publiez un événement au point de terminaison local.

Linux/macOS

Sous Linux et macOS, exécutez la commande `curl` suivante :

```
curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d '{}'
```

Cette commande invoque la fonction avec un événement vide et renvoie une réponse. Si vous utilisez votre propre code de fonction plutôt que l'exemple de code de fonction, vous pouvez invoquer la fonction avec une charge utile JSON. Exemple :

```
curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d
 '{"payload":"hello world!"}'
```

PowerShell

Dans PowerShell, exécutez la `Invoke-WebRequest` commande suivante :

```
Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/
invocations" -Method Post -Body '{}' -ContentType "application/json"
```

Cette commande invoque la fonction avec un événement vide et renvoie une réponse. Si vous utilisez votre propre code de fonction plutôt que l'exemple de code de fonction, vous pouvez invoquer la fonction avec une charge utile JSON. Exemple :

```
Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/
invocations" -Method Post -Body '{"payload":"hello world!"}' -ContentType
 "application/json"
```

4. Obtenez l'ID du conteneur.

```
docker ps
```

5. Utilisez la commande docker kill pour arrêter le conteneur. Dans cette commande, remplacez `3766c4ab331c` par l'ID du conteneur de l'étape précédente.

```
docker kill 3766c4ab331c
```

Déploiement de l'image

Pour charger l'image sur Amazon RIE et créer la fonction Lambda

1. Exécutez la commande get-login-password pour authentifier la CLI Docker auprès de votre registre Amazon ECR.

   - Définissez la `--region` valeur à l' Région AWS endroit où vous souhaitez créer le référentiel Amazon ECR.
   - `111122223333`Remplacez-le par votre Compte AWS identifiant.

   ```
   aws ecr get-login-password --region us-east-1 | docker login --username AWS --
   password-stdin 111122223333.dkr.ecr.us-east-1.amazonaws.com
   ```

2. Créez un référentiel dans Amazon ECR à l'aide de la commande create-repository.

   ```
   aws ecr create-repository --repository-name hello-world --region us-east-1 --image-
   scanning-configuration scanOnPush=true --image-tag-mutability MUTABLE
   ```

   > **Note**
   >
   > Le référentiel Amazon ECR doit être Région AWS identique à la fonction Lambda.

   En cas de succès, vous obtenez une réponse comme celle-ci :

   ```
   {
       "repository": {
           "repositoryArn": "arn:aws:ecr:us-east-1:111122223333:repository/hello-
   world",
           "registryId": "111122223333",
           "repositoryName": "hello-world",
           "repositoryUri": "111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-
   world",
           "createdAt": "2023-03-09T10:39:01+00:00",
           "imageTagMutability": "MUTABLE",
           "imageScanningConfiguration": {
               "scanOnPush": true
           },
           "encryptionConfiguration": {
   ```

```
            "encryptionType": "AES256"
        }
    }
}
```

3. Copiez le `repositoryUri` à partir de la sortie de l'étape précédente.
4. Exécutez la commande docker tag pour étiqueter votre image locale dans votre référentiel Amazon ECR en tant que dernière version. Dans cette commande :
   - `docker-image:test` est le nom et la balise de votre image Docker. Il s'agit du nom et de la balise de l'image que vous avez spécifiés dans la commande `docker build`.
   - Remplacez <ECRrepositoryUri> par l'`repositoryUri` que vous avez copié. Assurez-vous d'inclure `:latest` à la fin de l'URI.

```
docker tag docker-image:test <ECRrepositoryUri>:latest
```

   Exemple :

```
docker tag docker-image:test 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

5. Exécutez la commande docker push pour déployer votre image locale dans le référentiel Amazon ECR. Assurez-vous d'inclure `:latest` à la fin de l'URI du référentiel.

```
docker push 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

6. Créez un rôle d'exécution pour la fonction, si vous n'en avez pas déjà un. Vous aurez besoin de l'Amazon Resource Name (ARN) du rôle à l'étape suivante.
7. Créez la fonction Lambda. Pour `ImageUri`, indiquez l'URI du référentiel mentionné précédemment. Assurez-vous d'inclure `:latest` à la fin de l'URI.

```
aws lambda create-function \
  --function-name hello-world \
  --package-type Image \
  --code ImageUri=111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \
  --role arn:aws:iam::111122223333:role/lambda-ex
```

> **Note**
>
> Vous pouvez créer une fonction en utilisant une image d'un autre AWS compte, à condition que l'image se trouve dans la même région que la fonction Lambda. Pour plus d'informations, consultez Autorisations entre comptes Amazon ECR.

8. Invoquer la fonction.

```
aws lambda invoke --function-name hello-world response.json
```

Vous devriez obtenir une réponse comme celle-ci :

```
{
  "ExecutedVersion": "$LATEST",
  "StatusCode": 200
}
```

9. Pour voir la sortie de la fonction, consultez le fichier `response.json`.

Pour mettre à jour le code de la fonction, vous devez recréer l'image, charger la nouvelle image dans le référentiel Amazon ECR, puis utiliser la commande update-function-code pour déployer l'image dans la fonction Lambda.

Lambda résout l'étiquette d'image en hachage d'image spécifique. Cela signifie que si vous pointez la balise d'image qui a été utilisée pour déployer la fonction vers une nouvelle image dans Amazon ECR, Lambda ne met pas automatiquement à jour la fonction pour utiliser la nouvelle image.

Pour déployer la nouvelle image sur la même fonction Lambda, vous devez utiliser la commande update-function-code, même si la balise d'image dans Amazon ECR reste la même. Dans l'exemple suivant, l'option `--publish` crée une version de la fonction à l'aide de l'image du conteneur mise à jour.

```
aws lambda update-function-code \
  --function-name hello-world \
  --image-uri 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \
  --publish
```

Utilisation de couches pour les fonctions d'événement Ruby Lambda

Utilisez les couches Lambda pour empaqueter le code et les dépendances que vous souhaitez réutiliser dans plusieurs fonctions. Les couches contiennent généralement des dépendances de bibliothèque, une exécution personnalisée, ou des fichiers de configuration. La création d'une couche implique trois étapes générales :

1. Empaquetez le contenu de votre couche. Cela signifie créer une archive de fichiers .zip contenant les dépendances que vous souhaitez utiliser dans vos fonctions.
2. Créez la couche dans Lambda.
3. Ajoutez la couche à vos fonctions.

Rubriques

- Empaqueter le contenu de votre couche
- Créer la couche dans Lambda
- Utiliser des gems provenant de couches dans une fonction
- Ajouter la couche à votre fonction
- Exemple d'application

Empaqueter le contenu de votre couche

Pour créer une couche, regroupez vos packages dans une archive (fichier .zip) répondant aux exigences suivantes :

- Créez la couche à l'aide de la même version de Ruby que celle que vous prévoyez d'utiliser pour la fonction Lambda. Par exemple, si vous créez votre couche pour Ruby 4.0, utilisez le runtime Ruby 4.0 pour votre fonction.
- Le fichier .zip de votre couche doit utiliser l'une des structures de répertoires suivantes :
  - `ruby/gems/`*`x.x.x`* (où se *`x.x.x`* trouve votre version Ruby, par exemple `3.4.0`)
  - `ruby/lib`

  Pour plus d'informations, consultez Chemins d'accès de couche pour chaque exécution Lambda.
- Les packages de votre couche doivent être compatibles avec Linux. Les fonctions Lambda s'exécutent sur Amazon Linux.

Vous pouvez créer des couches contenant des gems Ruby tierces ou vos propres modules et classes Ruby. De nombreuses gems Ruby populaires contiennent des extensions natives (code C) qui doivent être compilées pour l'environnement Lambda Linux.

Gems Ruby pures

Les gems Ruby pures contiennent uniquement du code Ruby et ne nécessitent pas de compilation. Ces gems sont plus simples à empaqueter et à utiliser sur différentes plateformes.

Créer une couche à l'aide de gems Ruby pures

1. Créez un `Gemfile` pour spécifier les gems Ruby pures que vous souhaitez inclure dans votre couche :

   Example Gemfile

   ```
   source 'https://rubygems.org'

   gem 'tzinfo'
   ```

2. Installez les gems dans le répertoire `vendor/bundle` à l'aide de Bundler :

   ```
   bundle config set --local path vendor/bundle
   bundle install
   ```

3. Copiez les gems installées dans la structure de répertoires requise par Lambda (`ruby/gems/3.4.0`) :

   ```
   mkdir -p ruby/gems/3.4.0
   cp -r vendor/bundle/ruby/3.4.0*/* ruby/gems/3.4.0/
   ```

4. Compressez le contenu de la couche :

   Linux/macOS

   ```
   zip -r layer.zip ruby/
   ```

   PowerShell

   ```
   Compress-Archive -Path .\ruby -DestinationPath .\layer.zip
   ```

La structure de répertoire de votre fichier .zip devrait se présenter comme suit :

```
ruby/
### gems/
    ### 3.4.0/
        ### gems/
        #   ### concurrent-ruby-1.3.5/
        #   ### tzinfo-2.0.6/
        ### specifications/
        ### cache/
        ### build_info/
        ### (other bundler directories)
```

> **Note**
>
> Vous devez requérir chaque gem individuellement dans le code de votre fonction. Vous ne pouvez pas utiliser `bundler/setup` ou `Bundler.require`. Pour plus d'informations, consultez Utiliser des gems provenant de couches dans une fonction.

Gems avec des extensions natives

De nombreuses gems Ruby populaires contiennent des extensions natives (code C) qui doivent être compilées pour la plateforme cible. Les gems populaires dotées d'extensions natives incluent nokogiri, pg, mysql2, sqlite3, and ffi. Ces gems doivent être créées dans un environnement Linux compatible avec l'environnement d'exécution Lambda.

Créer une couche à l'aide de gems avec des extensions natives

1. Créez un `Gemfile`.

   Example Gemfile

   ```
   source 'https://rubygems.org'

   gem 'nokogiri'
   gem 'httparty'
   ```

2. Utilisez Docker pour créer les gems dans un environnement Linux compatible avec Lambda. Spécifiez une image de base AWS dans votre Dockerfile :

   Example Dockerfile pour Ruby 4.0

```
FROM public.ecr.aws/lambda/ruby:3.4

# Copy Gemfile
COPY Gemfile ./

# Install system dependencies for native extensions
RUN dnf update -y && \
    dnf install -y gcc gcc-c++ make

# Configure bundler and install gems
RUN bundle config set --local path vendor/bundle && \
    bundle install

# Create the layer structure
RUN mkdir -p ruby/gems/3.4.0 && \
    cp -r vendor/bundle/ruby/3.4.0*/* ruby/gems/3.4.0/

# Create the layer zip file
RUN zip -r layer.zip ruby/
```

3. Créez l'image et extrayez la couche :

```
docker build -t ruby-layer-builder .
docker run --rm -v $(pwd):/output --entrypoint cp ruby-layer-builder layer.zip /
output/
```

   Cela crée les gems dans l'environnement Linux approprié et copie le fichier `layer.zip` dans votre répertoire local. La structure de répertoire de votre fichier .zip devrait se présenter comme suit :

```
ruby/
### gems/
    ### 3.4.0/
        ### gems/
        #   ### bigdecimal-3.2.2/
        #   ### csv-3.3.5/
        #   ### httparty-0.23.1/
```

```
#   ### mini_mime-1.1.5/
#   ### multi_xml-0.7.2/
#   ### nokogiri-1.18.8-x86_64-linux-gnu/
#   ### racc-1.8.1/
### build_info/
### cache/
### specifications/
### (other bundler directories)
```

> **Note**
>
> Vous devez requérir chaque gem individuellement dans le code de votre fonction. Vous ne pouvez pas utiliser `bundler/setup` ou `Bundler.require`. Pour plus d'informations, consultez Utiliser des gems provenant de couches dans une fonction.

Modules Ruby personnalisés

Créer une couche à l'aide de votre propre code

1. Créez la structure de répertoires requise pour votre couche :

```
mkdir -p ruby/lib
```

2. Créez vos modules Ruby dans le répertoire `ruby/lib`. L'exemple de module suivant valide les commandes en confirmant qu'elles contiennent les informations requises.

   Example ruby/lib/order_validator.rb

```
require 'json'

module OrderValidator
  class ValidationError < StandardError; end

  def self.validate_order(order_data)
    # Validates an order and returns formatted data
    required_fields = %w[product_id quantity]

    # Check required fields
    missing_fields = required_fields.reject { |field| order_data.key?(field) }
    unless missing_fields.empty?
```

```
      raise ValidationError, "Missing required fields: #{missing_fields.join(',
 ')}"
    end

    # Validate quantity
    quantity = order_data['quantity']
    unless quantity.is_a?(Integer) && quantity > 0
      raise ValidationError, 'Quantity must be a positive integer'
    end

    # Format and return the validated data
    {
      'product_id' => order_data['product_id'].to_s,
      'quantity' => quantity,
      'shipping_priority' => order_data.fetch('priority', 'standard')
    }
  end

  def self.format_response(status_code, body)
    # Formats the API response
    {
      statusCode: status_code,
      body: JSON.generate(body)
    }
  end
end
```

3. Compressez le contenu de la couche :

   Linux/macOS

   ```
   zip -r layer.zip ruby/
   ```

   PowerShell

   ```
   Compress-Archive -Path .\ruby -DestinationPath .\layer.zip
   ```

   La structure de répertoire de votre fichier .zip devrait se présenter comme suit :

   ```
   ruby/
   ### lib/
   ```

```
    ### order_validator.rb
```

4. Dans votre fonction, exigez (require) et utilisez les modules. Vous devez requérir chaque gem individuellement dans le code de votre fonction. Vous ne pouvez pas utiliser `bundler/setup` ou `Bundler.require`. Pour plus d'informations, consultez Utiliser des gems provenant de couches dans une fonction. Exemple :

```
require 'json'
require 'order_validator'

def lambda_handler(event:, context:)
  begin
    # Parse the order data from the event body
    order_data = JSON.parse(event['body'] || '{}')

    # Validate and format the order
    validated_order = OrderValidator.validate_order(order_data)

    OrderValidator.format_response(200, {
      message: 'Order validated successfully',
      order: validated_order
    })
  rescue OrderValidator::ValidationError => e
    OrderValidator.format_response(400, {
      error: e.message
    })
  rescue => e
    OrderValidator.format_response(500, {
      error: 'Internal server error'
    })
  end
end
```

Vous pouvez utiliser l'événement de test suivant afin d'invoquer la fonction :

```
{
    "body": "{\"product_id\": \"ABC123\", \"quantity\": 2, \"priority\": \"express
\"}"
}
```

Réponse attendue :

```
{
  "statusCode": 200,
  "body": "{\"message\":\"Order validated successfully\",\"order\":{\"product_id\":
\"ABC123\",\"quantity\":2,\"shipping_priority\":\"express\"}}"
}
```

Créer la couche dans Lambda

Vous pouvez publier votre couche à l'aide de la console Lambda AWS CLI ou de la console Lambda.

AWS CLI

Exécutez la AWS CLI commande publish-layer-version pour créer la couche Lambda :

```
aws lambda publish-layer-version --layer-name my-layer --zip-file fileb://layer.zip
 --compatible-runtimes ruby4.0
```

Le paramètre compatible runtimes est facultatif. Lorsqu'il est spécifié, Lambda utilise ce paramètre pour filtrer les couches dans la console Lambda.

Console

Pour créer une couche (console)

1. Ouvrez la page Couches de la console Lambda.
2. Sélectionnez Créer un calque.
3. Choisissez Charger un fichier .zip, puis chargez l'archive .zip que vous avez créée précédemment.
4. (Facultatif) Pour Environnements d'exécution compatibles, choisissez l'environnement d'exécution Ruby qui correspond à la version de Ruby que vous avez utilisée pour créer votre couche.
5. Cliquez sur Créer.

Utiliser des gems provenant de couches dans une fonction

Dans le code de votre fonction, vous devez explicitement exiger chaque gem que vous souhaitez utiliser. Les commandes Bundler comme `bundler/setup` et `Bundler.require` ne sont pas prises en charge. Voici comment utiliser correctement les gems d'une couche dans une fonction Lambda :

```
# Correct: Use explicit requires for each gem
require 'nokogiri'
require 'httparty'

def lambda_handler(event:, context:)
  # Use the gems directly
  doc = Nokogiri::HTML(event['html'])
  response = HTTParty.get(event['url'])
  # ... rest of your function
end

# Incorrect: These Bundler commands will not work
# require 'bundler/setup'
# Bundler.require
```

Ajouter la couche à votre fonction

AWS CLI

Pour associer la couche à votre fonction, exécutez la commande update-function-configuration AWS CLI . Utilisez l'ARN de la couche pour le paramètre `--layers`. L'ARN doit spécifier la version (par exemple, `arn:aws:lambda:us-east-1:123456789012:layer:my-layer:1`). Pour plus d'informations, consultez Couches et versions de couches.

```
aws lambda update-function-configuration --function-name my-function --cli-binary-format raw-in-base64-out --layers "arn:aws:lambda:us-east-1:123456789012:layer:my-layer:1"
```

L'cli-binary-formatoption est obligatoire si vous utilisez AWS CLI la version 2. Pour faire de ce paramètre le paramètre par défaut, exécutez `aws configure set cli-binary-format raw-in-base64-out`. Pour plus d'informations, consultez les options de ligne de commande globales AWS CLI prises en charge dans le Guide de l'utilisateur AWS Command Line Interface version 2.

Console

Ajouter une couche à une fonction

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez la fonction.

3. Faites défiler jusqu'à la section Couches, puis choisissez Ajouter une couche.
4. Sous Choisir une couche, sélectionnez Couches personnalisées, puis choisissez votre couche.

> **Note**
>
> Si vous n'avez pas ajouté d'environnement d'exécution compatible lors de la création de la couche, celle-ci ne sera pas répertoriée ici. Vous pouvez spécifier l'ARN de la couche à la place.

5. Choisissez Ajouter.

Exemple d'application

Pour d'autres exemples d'utilisation des couches Lambda, consultez l'exemple d'application layer-ruby dans le référentiel du AWS Lambda Developer Guide. GitHub Cette application inclut une couche qui contient la bibliothèque tzinfo. Après avoir créé la couche, vous pouvez déployer et invoquer la fonction correspondante pour confirmer que la couche fonctionne comme prévu.

Utilisation de l'objet de contexte Lambda pour récupérer les informations de la fonction d'événement Ruby

Lorsque Lambda exécute votre fonction, il transmet un objet contexte au gestionnaire. Cet objet fournit des méthodes et des propriétés fournissant des informations sur l'invocation, la fonction et l'environnement d'exécution.

Méthodes de contexte

- `get_remaining_time_in_millis` – Renvoie le nombre de millisecondes restant avant l'expiration de l'exécution.

Propriétés du contexte

- `function_name` – Nom de la fonction Lambda.
- `function_version` – Version de la fonction.
- `invoked_function_arn` – Amazon Resource Name (ARN) utilisé pour appeler la fonction. Indique si l'appelant a spécifié un numéro de version ou un alias.
- `memory_limit_in_mb` – Quantité de mémoire allouée à la fonction.
- `aws_request_id` – Identifiant de la demande d'invocation.
- `log_group_name` – Groupe de journaux pour la fonction.
- `log_stream_name` – Flux de journal de l'instance de fonction.
- `deadline_ms` – Date d'expiration de l'exécution, exprimée en millisecondes au format horaire Unix.
- `identity` – (applications mobiles) Informations sur l'identité Amazon Cognito qui a autorisé la demande.
- `client_context` – (applications mobiles) Contexte client fourni à Lambda par l'application client.

Enregistrez et surveillez les fonctions d'événements Ruby Lambda

AWS Lambda surveille automatiquement les fonctions d'événement Lambda en votre nom et envoie les journaux à Amazon. CloudWatch Votre fonction est fournie avec un groupe de CloudWatch journaux Logs et un flux de journaux pour chaque instance de votre fonction. L'environnement d'exécution Lambda envoie des informations sur chaque invocation au flux de journaux et transmet les journaux et autres sorties provenant du code de votre fonction. Pour plus d'informations, consultez Envoi des journaux des fonctions d'événements Lambda aux journaux CloudWatch.

Cette page explique comment générer une sortie de journal à partir du code de votre fonction Lambda et comment accéder aux journaux à l'aide de la AWS Command Line Interface console Lambda ou de la console. CloudWatch

Sections

- Création d'une fonction qui renvoie des journaux
- Utilisation des contrôles de journalisation avancés de Lambda avec Ruby
- Affichage des journaux dans la console Lambda
- Afficher les journaux dans la CloudWatch console
- Afficher les journaux à l'aide du AWS Command Line Interface (AWS CLI)
- Suppression de journaux
- Utilisation de la bibliothèque Ruby logger

Création d'une fonction qui renvoie des journaux

Pour générer les journaux à partir de votre code de fonction, vous pouvez utiliser des déclarations `puts` ou n'importe quelle bibliothèque de journalisation qui écrit dans `stdout` ou `stderr`. L'exemple suivant consigne les valeurs des variables d'environnement et l'objet d'événement. Pour plus d'informations sur l'objet de contexte disponible pour votre gestionnaire, consultezthe section called "Contexte".

Example lambda_function.rb

```
# lambda_function.rb

def handler(event:, context:)
    puts "## ENVIRONMENT VARIABLES"
    puts ENV.to_a
```

```
    puts "## EVENT"
    puts event.to_a
end
```

Example format des journaux

```
START RequestId: 8f507cfc-xmpl-4697-b07a-ac58fc914c95 Version: $LATEST
## ENVIRONMENT VARIABLES
environ({'AWS_LAMBDA_LOG_GROUP_NAME': '/aws/lambda/my-function',
 'AWS_LAMBDA_LOG_STREAM_NAME': '2020/01/31/[$LATEST]3893xmpl7fac4485b47bb75b671a283c',
 'AWS_LAMBDA_FUNCTION_NAME': 'my-function', ...})
## EVENT
{'key': 'value'}
END RequestId: 8f507cfc-xmpl-4697-b07a-ac58fc914c95
REPORT RequestId: 8f507cfc-xmpl-4697-b07a-ac58fc914c95  Duration: 15.74 ms  Billed
 Duration: 147 ms Memory Size: 128 MB Max Memory Used: 56 MB  Init Duration: 130.49 ms
XRAY TraceId: 1-5e34a614-10bdxmplf1fb44f07bc535a1   SegmentId: 07f5xmpl2d1f6f85
 Sampled: true
```

L'exécution Ruby enregistre les lignes `START`, `END` et `REPORT` pour chaque invocation. La ligne de rapport fournit les détails suivants.

Champs de données de la ligne REPORT

- RequestId— L'identifiant de demande unique pour l'invocation.
- Duration – Temps que la méthode de gestion du gestionnaire de votre fonction a consacré au traitement de l'événement.
- Billed Duration : temps facturé pour l'invocation.
- Memory Size – Quantité de mémoire allouée à la fonction.
- Max Memory Used – Quantité de mémoire utilisée par la fonction. Lorsque les appels partagent un environnement d'exécution, Lambda indique la mémoire maximale utilisée pour toutes les invocations. Ce comportement peut entraîner une valeur signalée plus élevée que prévu.
- Init Duration : pour la première requête servie, temps qu'il a pris à l'exécution charger la fonction et exécuter le code en dehors de la méthode du gestionnaire.
- XRAY TraceId — Pour les demandes suivies, l'ID de AWS X-Ray trace.
- SegmentId— Pour les demandes suivies, l'ID X-Ray du segment.
- Sampled : pour les demandes suivies, résultat de l'échantillonnage.

Pour obtenir des journaux plus détaillés, utilisez la bibliothèque the section called “Utilisation de la bibliothèque Ruby logger”.

Utilisation des contrôles de journalisation avancés de Lambda avec Ruby

Pour vous permettre de mieux contrôler la manière dont les journaux de vos fonctions sont capturés, traités et consommés, Lambda propose des contrôles de journalisation avancés avec Ruby. Pour les environnements d'exécution de Ruby 4.0 et versions ultérieures, vous pouvez configurer les options de journalisation suivantes :

- Format de journal : choisissez entre le format texte brut et le format JSON structuré pour les journaux de votre fonction
- Niveau de journalisation : pour les journaux au format JSON, choisissez le niveau de détail des journaux que Lambda envoie à Amazon CloudWatch, par exemple ERROR, DEBUG ou INFO
- Groupe de journaux : choisissez le groupe de CloudWatch journaux auquel votre fonction envoie les journaux

Pour plus d’informations sur ces options de journalisation et pour savoir comment configurer votre fonction pour les utiliser, consultez the section called “Configuration de contrôles de journalisation avancés pour les fonctions d'événement Lambda”.

Pour en savoir plus sur l'utilisation du format de journal et des options de niveau de journal avec vos fonctions Ruby Lambda, consultez les instructions des sections suivantes.

Utilisation de journaux JSON structurés avec Ruby

Si vous sélectionnez JSON pour le format de journal de votre fonction, Lambda enverra les journaux produits par la `Logger` bibliothèque standard Ruby au CloudWatch format JSON structuré. Chaque objet de journal JSON contient au moins quatre paires clé-valeur avec les clés suivantes :

- `"timestamp"` - heure à laquelle le message de journal a été généré
- `"level"` - niveau de journalisation attribué au message
- `"message"` - contenu du message de journal
- `"requestId"` - identifiant unique de la demande pour l’invocation de la fonction

La `Logger` bibliothèque Ruby peut également ajouter des paires clé-valeur supplémentaires, comme dans `"logger"` cet objet JSON.

Les exemples présentés dans les sections suivantes montrent comment les sorties de journal générées à l'aide de la `Logger` bibliothèque Ruby sont capturées dans CloudWatch Logs lorsque vous configurez le format de journal de votre fonction au format JSON.

Notez que si vous utilisez la `puts` méthode pour produire des sorties de journal de base comme décrit dansthe section called “Création d’une fonction qui renvoie des journaux”, Lambda capturera ces sorties sous forme de texte brut, même si vous configurez le format de journalisation de votre fonction au format JSON.

Sorties de journal JSON standard à l'aide de la bibliothèque Ruby Logger

Les exemples d'extrait de code et de sortie de journal suivants montrent comment les sorties de journal standard générées à l'aide de la `Logger` bibliothèque Ruby sont capturées dans CloudWatch Logs lorsque le format de journal de votre fonction est défini sur JSON.

Example Exemple de code de journalisation Ruby

```
require 'logger'

def lambda_handler(event:, context:)
  logger = Logger.new($stdout)
  logger.info("Inside the handler function")
end
```

Example Exemple d'enregistrement de journal JSON

```
{
    "timestamp": "2025-10-27T19:17:45.586Z",
    "level": "INFO",
    "message": "Inside the handler function",
    "requestId": "79b4f56e-95b1-4643-9700-2807f4e68189"
}
```

Enregistrement de paramètres supplémentaires au format JSON

Lorsque le format de journal de votre fonction est défini sur JSON, vous pouvez également enregistrer des paramètres supplémentaires avec la `Logger` bibliothèque Ruby en transmettant un hachage de paires clé-valeur supplémentaires à la sortie du journal.

Example Exemple de code de journalisation Ruby

```
require 'logger'
```

```
require 'json'

def lambda_handler(event:, context:)
  logger = Logger.new($stdout)
  extra_params = { "a" => "b", "b" => [3] }
  logger.info({ message: "extra parameters example" }.merge(extra_params).to_json)
end
```

Example Exemple d'enregistrement de journal JSON

```
{
    "timestamp": "2025-11-02T15:26:28Z",
    "level": "INFO",
    "message": "extra parameters example",
    "requestId": "3dbd5759-65f6-45f8-8d7d-5bdc79a3bd01",
    "a": "b",
    "b": [
        3
    ]
}
```

Exceptions de journalisation au format JSON

L'extrait de code suivant montre comment les exceptions Ruby sont capturées dans la sortie du journal de votre fonction lorsque vous configurez le format de journal au format JSON. Notez que les sorties de journal générées à l'`logger.error`aide d'une exception se voient attribuer le niveau de journal ERROR.

Example Exemple de code de journalisation Ruby

```
require 'logger'

def lambda_handler(event:, context:)
  logger = Logger.new($stdout)
  begin
    raise "exception"
  rescue => e
    logger.error(e)
  end
end
```

Example Exemple d'enregistrement de journal JSON

```
{
    "timestamp": "2025-11-02T16:18:57Z",
    "level": "ERROR",
    "message": "exception",
    "stackTrace": [
        "  /var/task/lambda_function.rb:4:in `lambda_handler'"
    ],
    "errorType": "RuntimeError",
    "errorMessage": "exception",
    "requestId": "3f9d155c-0f09-46b7-bdf1-e91dab220855",
    "location": "/var/task/lambda_function.rb:lambda_handler:6"
}
```

Utilisation du filtrage au niveau du journal avec Ruby

En configurant le filtrage au niveau des journaux, vous pouvez choisir de n'envoyer que les journaux ayant un certain niveau de journalisation ou un niveau inférieur à CloudWatch Logs. Pour savoir comment configurer le filtrage de niveau journal de votre fonction, consultez the section called “Log-level filtrage”.

AWS Lambda Pour filtrer les journaux de votre application en fonction de leur niveau de journalisation, votre fonction doit utiliser des journaux au format JSON. Vous pouvez effectuer cette opération de deux façons :

- Créez des sorties de journal à l'aide de la `Logger` bibliothèque Ruby standard et configurez votre fonction pour utiliser le format de journal JSON. AWS Lambda filtre ensuite les sorties de votre journal à l'`'"level"` aide de la paire clé-valeur de l'objet JSON décrit dansthe section called “Utilisation de journaux JSON structurés avec Ruby”. Pour savoir comment configurer le format de journal de votre fonction, consultezthe section called “Configuration de contrôles de journalisation avancés pour les fonctions d'événement Lambda”.
- Utilisez une autre bibliothèque ou méthode de journalisation pour créer des journaux structurés JSON dans votre code qui incluent une `"level"` paire clé-valeur définissant le niveau de sortie du journal.

Vous pouvez également utiliser une `puts` instruction pour générer un objet JSON contenant un identifiant de niveau de journalisation. L'`puts`instruction suivante produit une sortie au format JSON dans laquelle le niveau de journalisation est défini sur INFO. AWS Lambda enverra l'objet JSON

à CloudWatch Logs si le niveau de journalisation de votre fonction est défini sur INFO, DEBUG ou TRACE.

```
puts '{"msg":"My log message", "level":"info"}'
```

Pour que Lambda puisse filtrer les journaux de votre fonction, vous devez également inclure une paire `"timestamp"` clé-valeur dans la sortie de votre journal JSON. L'heure doit être spécifiée dans un format d'horodatage RFC 3339 valide. Si vous ne fournissez pas d'horodatage valide, Lambda attribuera au journal le niveau INFO et ajoutera un horodatage pour vous.

Utilisation d'une autre bibliothèque de journalisation

Si vous devez utiliser une version personnalisée de la `logger` bibliothèque, vous pouvez l'inclure dans votre package de déploiement ou dans une couche Lambda, et définir la variable d'`RUBYLIB`environnement sur le répertoire de `lib` la bibliothèque. Le moteur d'exécution Lambda chargera votre version au lieu de celle fournie.

Si votre code utilise déjà une autre bibliothèque de journalisation pour produire des journaux structurés en JSON, vous n'avez pas besoin d'apporter de modifications. AWS Lambda ne double code aucun journal déjà codé au format JSON. Même si vous configurez votre fonction pour utiliser le format de journal JSON, vos sorties de journalisation apparaissent CloudWatch dans la structure JSON que vous définissez.

Affichage des journaux dans la console Lambda

Vous pouvez utiliser la console Lambda pour consulter les résultats du journal après avoir invoqué une fonction d'événement Lambda.

Si votre code peut être testé à partir de l'éditeur de code intégré, vous trouverez des journaux dans les résultats d'exécution. Lorsque vous utilisez la fonctionnalité de test de la console pour appeler une fonction, vous trouverez la sortie du journal dans la section Détails.

Afficher les journaux dans la CloudWatch console

Vous pouvez utiliser la CloudWatch console Amazon pour consulter les journaux de toutes les invocations de la fonction d'événement Lambda.

Pour afficher les journaux sur la CloudWatch console

1. Ouvrez la page Groupes de journaux sur la CloudWatch console.

2. Choisissez le groupe de journaux pour votre fonction (/aws/lambda/***your-function-name***).
3. Choisissez un flux de journaux.

Chaque flux de journal correspond à une instance de votre fonction. Un flux de journal apparaît lorsque vous mettez à jour votre fonction Lambda et lorsque des instances supplémentaires sont créées pour gérer les appels simultanés. Pour trouver les journaux d'un appel spécifique, nous vous recommandons d'instrumenter votre fonction avec. AWS X-Ray X-Ray enregistre les détails de la demande et du flux de log dans le traçage.

Afficher les journaux à l'aide du AWS Command Line Interface (AWS CLI)

AWS CLI Il s'agit d'un outil open source que vous pouvez utiliser pour interagir avec les AWS services à l'aide de commandes dans votre interface de ligne de commande. Pour effectuer les étapes de cette section, vous devez disposer de la version 2 de l'AWS CLI.

Vous pouvez utiliser AWS CLI pour récupérer les journaux d'une invocation à l'aide de l'option de commande `--log-type`. La réponse inclut un champ `LogResult` qui contient jusqu'à 4 Ko de journaux codés en base64 provenant de l'invocation.

Example récupérer un ID de journal

L'exemple suivant montre comment récupérer un ID de journal à partir du champ `LogResult` d'une fonction nommée `my-function`.

```
aws lambda invoke --function-name my-function out --log-type Tail
```

Vous devriez voir la sortie suivante:

```
{
    "StatusCode": 200,
    "LogResult":
 "U1RBUlQgUmVxdWVzdElkOiA4N2QwNDRiOC1mMTU0LTExZTgtOGNkYS0yOTc0YzVlNGZiMjEgVmVyc2lvb...",
    "ExecutedVersion": "$LATEST"
}
```

Example décoder les journaux

Dans la même invite de commandes, utilisez l'utilitaire `base64` pour décoder les journaux. L'exemple suivant montre comment récupérer les journaux encodés en base64 pour `my-function`.

```
aws lambda invoke --function-name my-function out --log-type Tail \
--query 'LogResult' --output text --cli-binary-format raw-in-base64-out | base64 --
decode
```

L'cli-binary-formatoption est obligatoire si vous utilisez AWS CLI la version 2. Pour faire de ce paramètre le paramètre par défaut, exécutez `aws configure set cli-binary-format raw-in-base64-out`. Pour plus d'informations, consultez les options de ligne de commande globales AWS CLI prises en charge dans le Guide de l'utilisateur AWS Command Line Interface version 2.

Vous devriez voir la sortie suivante :

```
START RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8 Version: $LATEST
"AWS_SESSION_TOKEN": "AgoJb3JpZ2luX2VjELj...", "_X_AMZN_TRACE_ID": "Root=1-5d02e5ca-
f5792818b6fe8368e5b51d50;Parent=191db58857df8395;Sampled=0"",ask/lib:/opt/lib",
END RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8
REPORT RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8  Duration: 79.67 ms      Billed
 Duration: 80 ms         Memory Size: 128 MB     Max Memory Used: 73 MB
```

L'utilitaire `base64` est disponible sous Linux, macOS et Ubuntu sous Windows. Les utilisateurs de macOS auront peut-être besoin d'utiliser `base64 -D`.

Example Script get-logs.sh

Dans la même invite de commandes, utilisez le script suivant pour télécharger les cinq derniers événements de journalisation. Le script utilise `sed` pour supprimer les guillemets du fichier de sortie et attend 15 secondes pour permettre la mise à disposition des journaux. La sortie comprend la réponse de Lambda, ainsi que la sortie de la commande `get-log-events`.

Copiez le contenu de l'exemple de code suivant et enregistrez-le dans votre répertoire de projet Lambda sous `get-logs.sh`.

L'cli-binary-formatoption est obligatoire si vous utilisez AWS CLI la version 2. Pour faire de ce paramètre le paramètre par défaut, exécutez `aws configure set cli-binary-format raw-in-base64-out`. Pour plus d'informations, consultez les options de ligne de commande globales AWS CLI prises en charge dans le Guide de l'utilisateur AWS Command Line Interface version 2.

```
#!/bin/bash
aws lambda invoke --function-name my-function --cli-binary-format raw-in-base64-out --
payload '{"key": "value"}' out
sed -i'' -e 's/"//g' out
```

```
sleep 15
aws logs get-log-events --log-group-name /aws/lambda/my-function --log-stream-
name stream1 --limit 5
```

Example macOS et Linux (uniquement)

Dans la même invite de commande, les utilisateurs de macOS et de Linux devront peut-être exécuter la commande suivante pour s'assurer que le script est exécutable.

```
chmod -R 755 get-logs.sh
```

Example récupérer les cinq derniers événements de journal

Dans la même invite de commande, exécutez le script suivant pour obtenir les cinq derniers événements de journalisation.

```
./get-logs.sh
```

Vous devriez voir la sortie suivante:

```
{
    "StatusCode": 200,
    "ExecutedVersion": "$LATEST"
}
{
    "events": [
        {
            "timestamp": 1559763003171,
            "message": "START RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf Version:
 $LATEST\n",
            "ingestionTime": 1559763003309
        },
        {
            "timestamp": 1559763003173,
            "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tENVIRONMENT VARIABLES\r{\r  \"AWS_LAMBDA_FUNCTION_VERSION\": \"$LATEST\",
\r ...",
            "ingestionTime": 1559763018353
        },
        {
            "timestamp": 1559763003173,
```

```
            "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tEVENT\r{\r  \"key\": \"value\"\r}\n",
            "ingestionTime": 1559763018353
        },
        {
            "timestamp": 1559763003218,
            "message": "END RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf\n",
            "ingestionTime": 1559763018353
        },
        {
            "timestamp": 1559763003218,
            "message": "REPORT RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tDuration: 26.73 ms\tBilled Duration: 27 ms \tMemory Size: 128 MB\tMax Memory Used: 75
 MB\t\n",
            "ingestionTime": 1559763018353
        }
    ],
    "nextForwardToken": "f/34783877304859518393868359594929986069206639495374241795",
    "nextBackwardToken": "b/34783877303811383369537420289090800615709599058929582080"
}
```

Suppression de journaux

Les groupes de journaux ne sont pas supprimés automatiquement quand vous supprimez une fonction. Pour éviter de stocker des journaux indéfiniment, supprimez le groupe de journaux ou configurez une période de conservation à l'issue de laquelle les journaux sont supprimés automatiquement.

Utilisation de la bibliothèque Ruby logger

La bibliothèque Ruby logger renvoie des journaux simplifiés, faciles à lire. Utilisez l'utilitaire logger pour obtenir des informations détaillées, des messages et des codes d'erreur relatifs à votre fonction.

```
# lambda_function.rb

require 'logger'

def handler(event:, context:)
  logger = Logger.new($stdout)
  logger.info('## ENVIRONMENT VARIABLES')
  logger.info(ENV.to_a)
  logger.info('## EVENT')
  logger.info(event)
```

```
  event.to_a
end
```

La sortie de `logger` inclut le niveau de journal, l'horodatage et l'ID de demande.

```
START RequestId: 1c8df7d3-xmpl-46da-9778-518e6eca8125 Version: $LATEST
[INFO]  2020-01-31T22:12:58.534Z    1c8df7d3-xmpl-46da-9778-518e6eca8125    ##
 ENVIRONMENT VARIABLES

[INFO]  2020-01-31T22:12:58.534Z    1c8df7d3-xmpl-46da-9778-518e6eca8125
    environ({'AWS_LAMBDA_LOG_GROUP_NAME': '/aws/lambda/my-function',
 'AWS_LAMBDA_LOG_STREAM_NAME': '2020/01/31/[$LATEST]1bbe51xmplb34a2788dbaa7433b0aa4d',
 'AWS_LAMBDA_FUNCTION_NAME': 'my-function', ...})

[INFO]  2020-01-31T22:12:58.535Z    1c8df7d3-xmpl-46da-9778-518e6eca8125    ## EVENT

[INFO]  2020-01-31T22:12:58.535Z    1c8df7d3-xmpl-46da-9778-518e6eca8125    {'key':
 'value'}

END RequestId: 1c8df7d3-xmpl-46da-9778-518e6eca8125
REPORT RequestId: 1c8df7d3-xmpl-46da-9778-518e6eca8125  Duration: 2.75 ms   Billed
 Duration: 117 ms Memory Size: 128 MB Max Memory Used: 56 MB  Init Duration: 113.51 ms
XRAY TraceId: 1-5e34a66a-474xmpl7c2534a87870b4370   SegmentId: 073cxmpl3e442861
 Sampled: true
```

Instrumentation du code Ruby dans AWS Lambda

Lambda s'intègre AWS X-Ray pour vous permettre de suivre, de déboguer et d'optimiser les applications Lambda. Vous pouvez utiliser X-Ray pour suivre une demande lorsqu'elle qu'elle parcourt les ressources de votre application, de l'API frontale au stockage et à la base de données sur le backend. En ajoutant simplement la bibliothèque du X-Ray SDK à votre configuration de build, vous pouvez enregistrer les erreurs et le temps de latence pour chaque appel effectué par votre fonction à un AWS service.

Une fois que vous avez configuré le suivi actif, vous pouvez observer des demandes spécifiques via votre application. Le graphique X-Ray de service affiche des informations sur votre application et tous ses composants. L'exemple suivant montre une application dotée de deux fonctions. La fonction principale traite les événements et renvoie parfois des erreurs. La deuxième fonction située en haut traite les erreurs qui apparaissent dans le groupe de journaux de la première et utilise le AWS SDK pour appeler X-Ray Amazon Simple Storage Service (Amazon S3) et Amazon Logs. CloudWatch

Pour activer le suivi actif de votre fonction d'événement Lambda à l'aide de la console, procédez comme suit :

Pour activer le traçage actif

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez une fonction d'événement.
3. Choisissez Configuration, puis choisissez Outils de surveillance et d'opérations.
4. Dans Outils de surveillance supplémentaires, choisissez Modifier.

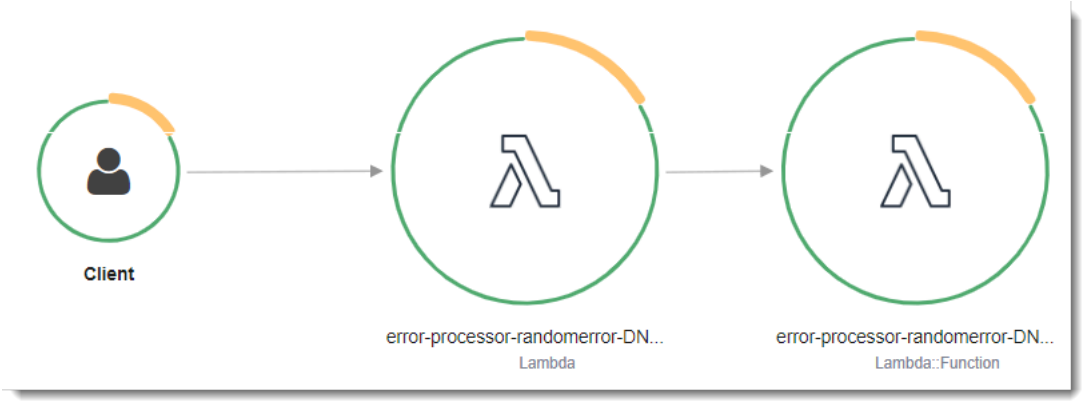
5. Sous Signaux CloudWatch d'application et AWS X-Ray sélectionnez Activer les traces de service Lambda.
6. Cliquez sur Enregistrer.

> **Tarification**
>
> Vous pouvez utiliser le X-Ray suivi gratuitement chaque mois jusqu'à une certaine limite dans le cadre du niveau AWS gratuit. Au-delà de ce seuil, les X-Ray frais de stockage et de récupération des traces sont facturés. Pour en savoir plus, consultez Pricing AWS X-Ray (Tarification).

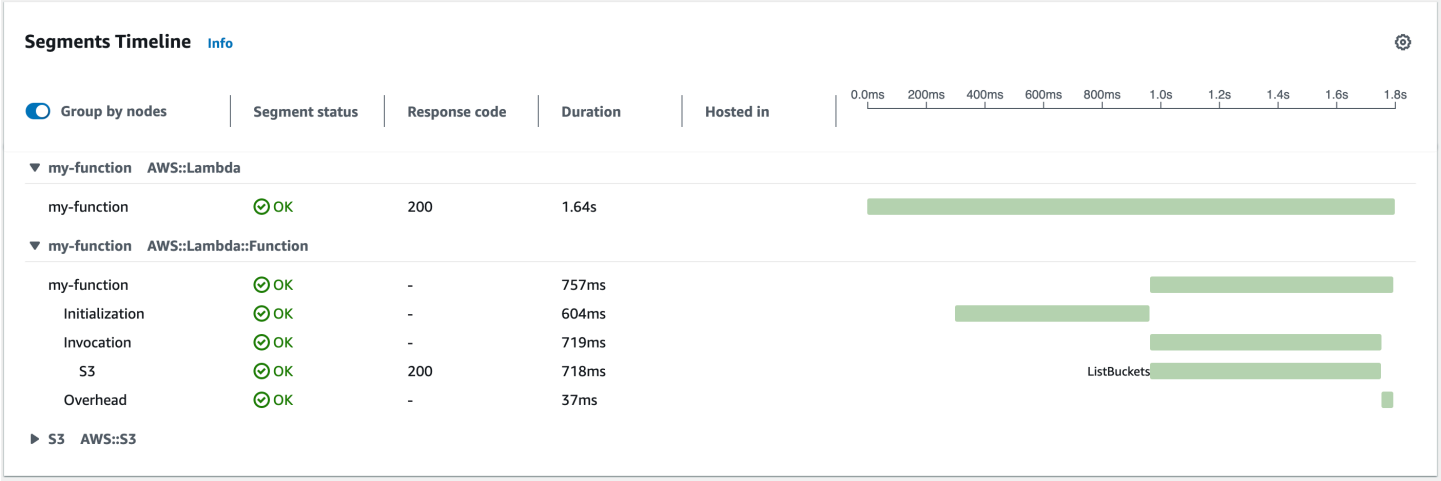
Votre fonction événementielle a besoin d'une autorisation pour télécharger des données de suivi sur X-Ray. Lorsque vous activez le suivi dans la console Lambda, Lambda ajoute les autorisations requises au rôle d'exécution de votre fonction d'événement. Dans le cas contraire, ajoutez la AWSXRayDaemonWriteAccesspolitique au rôle d'exécution.

X-Ray n'assure pas le suivi de toutes les demandes jusqu'à votre application. X-Ray applique un algorithme d'échantillonnage pour garantir l'efficacité du suivi, tout en fournissant un échantillon représentatif de toutes les demandes. Le taux d'échantillonnage est 1 demande par seconde et 5 % de demandes supplémentaires. Vous ne pouvez pas configurer le taux X-Ray d'échantillonnage pour vos fonctions.

Dans X-Ray, un suivi enregistre des informations relatives à une demande traitée par un ou plusieurs services. Lambda enregistre deux segments par suivi, ce qui a pour effet de créer deux nœuds sur le graphique du service. L'image suivante met en évidence ces deux nœuds :



Le premier nœud sur la gauche représente le service Lambda qui reçoit la demande d'invocation. Le deuxième nœud représente votre fonction Lambda spécifique. L'exemple suivant illustre une trace avec ces deux segments. Les deux sont nommés my-function, mais l'un a pour origine `AWS::Lambda` et l'autre a pour origine `AWS::Lambda::Function`. Si le segment `AWS::Lambda` affiche une erreur, cela signifie que le service Lambda a rencontré un problème. Si le segment `AWS::Lambda::Function` affiche une erreur, cela signifie que votre fonction a rencontré un problème.



Cet exemple développe le segment `AWS::Lambda::Function` pour afficher ses trois sous-segments.

> **Note**
>
> AWS met actuellement en œuvre des modifications du service Lambda. En raison de ces modifications, vous pouvez constater des différences mineures entre la structure et le contenu des messages du journal système et des segments de trace émis par les différentes fonctions d'événement Lambda de votre ordinateur. Compte AWS
> L'exemple de suivi présenté ici illustre le segment de fonction à l'ancienne. Les différences entre les segments à l'ancienne et de style moderne sont décrites dans les paragraphes suivants.
> Ces modifications seront mises en œuvre au cours des prochaines semaines, et toutes les fonctions, Régions AWS sauf en Chine et dans les GovCloud régions, seront transférées pour utiliser le nouveau format des messages de journal et des segments de trace.

Le segment de fonction à l'ancienne contient les sous-segments suivants :

- Initialization (Initialisation) : représente le temps passé à charger votre fonction et à exécuter le code d'initialisation. Ce sous-segment apparaît pour le premier événement traité par chaque instance de votre fonction.
- Invocation – Représente le temps passé à exécuter votre code de gestionnaire.
- Overhead (Travail supplémentaire) – Représente le temps que le fichier d'exécution Lambda passe à se préparer à gérer l'événement suivant.

Le segment de fonction de style moderne ne contient pas de sous-segment `Invocation`. À la place, les sous-segments du client sont directement rattachés au segment de fonction. Pour plus d'informations sur la structure des segments de fonction à l'ancienne et de style moderne, consultez the section called "Comprendre les X-Ray traces".

Vous pouvez instrumenter le code de gestionnaire pour enregistrer les métadonnées et suivre les appels en aval. Pour enregistrer les détails des appels que votre gestionnaire fait à d'autres ressources et services, utilisez le X-Ray SDK for Ruby. Pour obtenir ce kit SDK, ajoutez le package `aws-xray-sdk` aux dépendances de votre application.

Example fichier ruby/function blanche/Gemfile

```
# Gemfile
source 'https://rubygems.org'

gem 'aws-xray-sdk', '0.11.4'
gem 'aws-sdk-lambda', '1.39.0'
gem 'test-unit', '3.3.5'
```

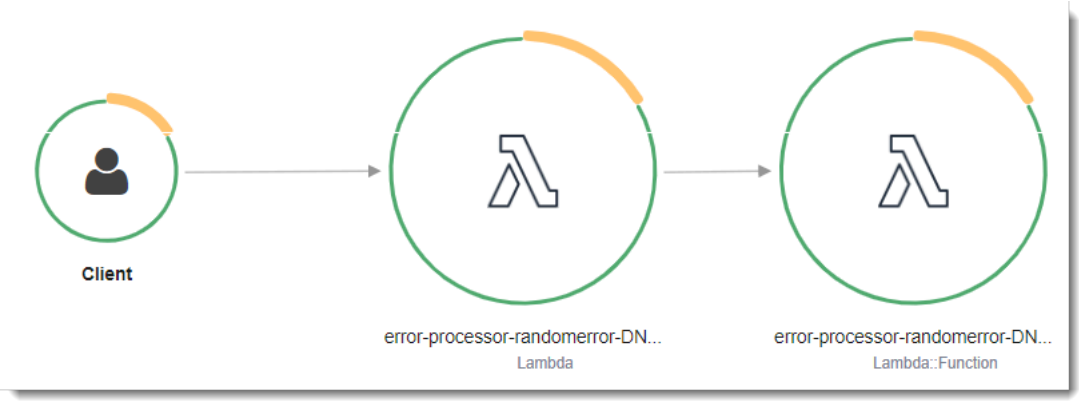
Pour instrumenter les clients du AWS SDK, vous devez avoir besoin du `aws-xray-sdk/lambda` module après avoir créé un client dans le code d'initialisation.

Example blank- ruby/function /lambda_function.rb — Tracer un AWS Client du SDK

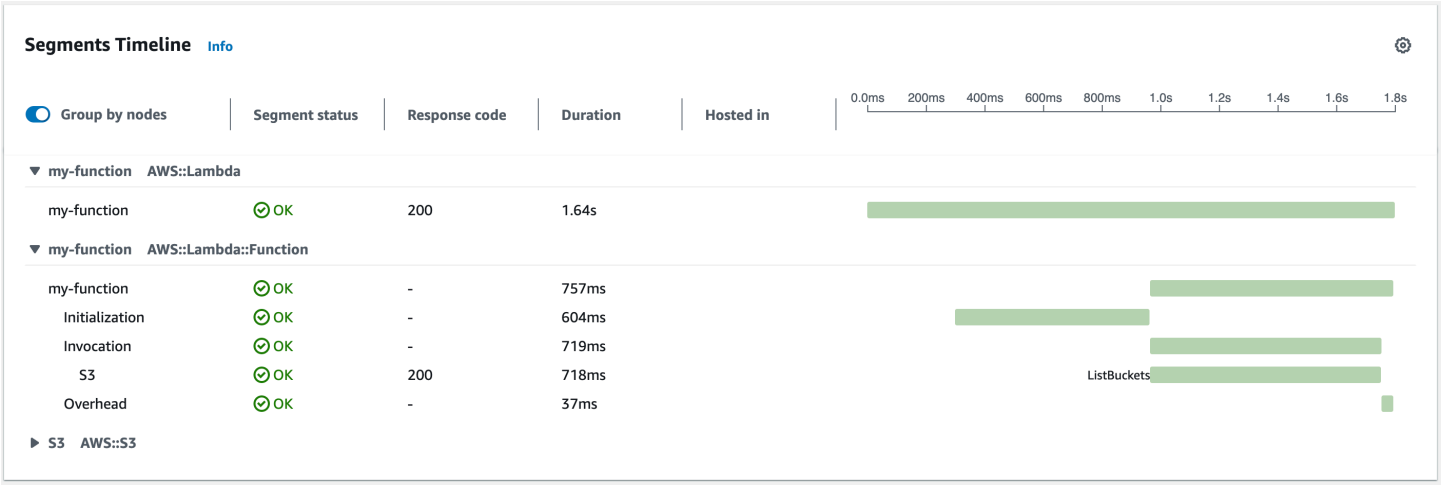
```
# lambda_function.rb
require 'logger'
require 'json'
require 'aws-sdk-lambda'
$client = Aws::Lambda::Client.new()
$client.get_account_settings()

require 'aws-xray-sdk/lambda'
```

```
def lambda_handler(event:, context:)
  logger = Logger.new($stdout)
  ...
```

Dans X-Ray, un suivi enregistre des informations relatives à une demande traitée par un ou plusieurs services. Lambda enregistre deux segments par suivi, ce qui a pour effet de créer deux nœuds sur le graphique du service. L'image suivante met en évidence ces deux nœuds :



Le premier nœud sur la gauche représente le service Lambda qui reçoit la demande d'invocation. Le deuxième nœud représente votre fonction Lambda spécifique. L'exemple suivant illustre une trace avec ces deux segments. Les deux sont nommés my-function, mais l'un a pour origine `AWS::Lambda` et l'autre a pour origine `AWS::Lambda::Function`. Si le segment `AWS::Lambda` affiche une erreur, cela signifie que le service Lambda a rencontré un problème. Si le segment `AWS::Lambda::Function` affiche une erreur, cela signifie que votre fonction a rencontré un problème.



Cet exemple développe le segment `AWS::Lambda::Function` pour afficher ses trois sous-segments.

> **Note**
>
> AWS met actuellement en œuvre des modifications du service Lambda. En raison de ces modifications, vous pouvez constater des différences mineures entre la structure et le contenu des messages du journal système et des segments de trace émis par les différentes fonctions d'événement Lambda de votre ordinateur. Compte AWS
> L'exemple de suivi présenté ici illustre le segment de fonction à l'ancienne. Les différences entre les segments à l'ancienne et de style moderne sont décrites dans les paragraphes suivants.
> Ces modifications seront mises en œuvre au cours des prochaines semaines, et toutes les fonctions, Régions AWS sauf en Chine et dans les GovCloud régions, seront transférées pour utiliser le nouveau format des messages de journal et des segments de trace.

Le segment de fonction à l'ancienne contient les sous-segments suivants :

- Initialization (Initialisation) : représente le temps passé à charger votre fonction et à exécuter le code d'initialisation. Ce sous-segment apparaît pour le premier événement traité par chaque instance de votre fonction.
- Invocation – Représente le temps passé à exécuter votre code de gestionnaire.
- Overhead (Travail supplémentaire) – Représente le temps que le fichier d'exécution Lambda passe à se préparer à gérer l'événement suivant.

Le segment de fonction de style moderne ne contient pas de sous-segment `Invocation`. À la place, les sous-segments du client sont directement rattachés au segment de fonction. Pour plus d'informations sur la structure des segments de fonction à l'ancienne et de style moderne, consultez the section called "Comprendre les X-Ray traces".

Vous pouvez également utiliser des clients HTTP, enregistrer des requêtes SQL et créer des sous-segments personnalisés avec des annotations et des métadonnées. Pour plus d'informations, consultez le X-Ray SDK pour Ruby dans AWS X-Ray le manuel du développeur.

Sections

- Activation du suivi actif avec l'API Lambda
- Activation du suivi actif avec CloudFormation
- Stockage des dépendances d'exécution dans une couche

Activation du suivi actif avec l'API Lambda

Pour gérer la configuration du suivi avec le AWS SDK AWS CLI ou le SDK, utilisez les opérations d'API suivantes :

- UpdateFunctionConfiguration
- GetFunctionConfiguration
- CreateFunction

L'exemple de AWS CLI commande suivant active le suivi actif sur une fonction nommée my-function.

```
aws lambda update-function-configuration --function-name my-function \
--tracing-config Mode=Active
```

Le mode de suivi fait partie de la configuration spécifique de la version lorsque vous publiez une version de votre fonction. Vous ne pouvez pas modifier le mode de suivi sur une version publiée.

Activation du suivi actif avec CloudFormation

Pour activer le suivi d'une `AWS::Lambda::Function` ressource dans un CloudFormation modèle, utilisez la `TracingConfig` propriété.

Example fonction-inline.yml — Configuration du suivi

```
Resources:
  function:
    Type: AWS::Lambda::Function
    Properties:
      TracingConfig:
        Mode: Active
      ...
```

Pour une `AWS::Serverless::Function` ressource AWS Serverless Application Model (AWS SAM), utilisez la `Tracing` propriété.

Example template.yml — Configuration du suivi

```
Resources:
  function:
    Type: AWS::Serverless::Function
```

```
    Properties:
      Tracing: Active
      ...
```

Stockage des dépendances d'exécution dans une couche

Si vous utilisez le X-Ray SDK pour instrumenter le code de fonction des clients du AWS SDK, votre package de déploiement peut devenir assez volumineux. Pour éviter de télécharger les dépendances d'exécution chaque fois que vous mettez à jour le code de votre fonction, empaquetez le X-Ray SDK dans une couche Lambda.

L'exemple suivant montre une `AWS::Serverless::LayerVersion` ressource qui stocke le X-Ray SDK for Ruby.

Example template.yml — Couche de dépendances

```
Resources:
  function:
    Type: AWS::Serverless::Function
    Properties:
      CodeUri: function/.
      Tracing: Active
      Layers:
        - !Ref libs
      ...
  libs:
    Type: AWS::Serverless::LayerVersion
    Properties:
      LayerName: blank-ruby-lib
      Description: Dependencies for the blank-ruby sample app.
      ContentUri: lib/.
      CompatibleRuntimes:
        - ruby2.5
```

Avec cette configuration, vous ne mettez à jour les fichiers de couche de bibliothèque que si vous modifiez vos dépendances d'exécution. Étant donné que le package de déploiement de la fonction contient uniquement votre code, cela peut contribuer à réduire les temps de chargement.

La création d'une couche pour les dépendances nécessite des modifications de construction pour générer l'archive de couches avant le déploiement. Pour un exemple fonctionnel, consultez l'exemple d'application blank-ruby.

Création de fonctions d'événement Lambda avec Java

Vous pouvez exécuter du code Java dans AWS Lambda Event Functions. Lambda fournit des runtimes pour Java qui exécutent votre code afin de traiter des événements. Votre code s'exécute dans un environnement Amazon Linux qui inclut les AWS informations d'identification d'un rôle Gestion des identités et des accès AWS (IAM) que vous gérez.

Lambda prend en charge les environnements d'exécution Java suivants.

Nom	Identifiant	Système d'exploitation	Date d'obsolescence	Créer la fonction de blocage	Mettre à jour la fonction de blocage
Java 25	`java25`	Amazon Linux 2	30 juin 2029	31 juillet 2029	31 août 2029
Java 21	`java21`	Amazon Linux 2	30 juin 2029	31 juillet 2029	31 août 2029
Java 17	`java17.al2023`	Amazon Linux 2	30 juin 2029	31 juillet 2029	31 août 2029
Java 11	`java11.al2023`	Amazon Linux 2	30 juin 2029	31 juillet 2029	31 août 2029
Java 8	`java8.al2023`	Amazon Linux 2	30 juin 2029	31 juillet 2029	31 août 2029
Java 17	`java17`	Amazon Linux 2	30 juin 2027	29 juillet 2027	31 août 2027
Java 11	`java11`	Amazon Linux 2	30 juin 2027	29 juillet 2027	31 août 2027
Java 8	`java8.al2`	Amazon Linux 2	30 juin 2027	29 juillet 2027	31 août 2027

AWS fournit les bibliothèques suivantes pour les fonctions Java. Ces bibliothèques sont disponibles via le Référentiel central Maven.

- com.amazonaws:aws-lambda-java-core (obligatoire) – Définit les interfaces de méthode du gestionnaire et l'objet contexte que l'environnement d'exécution transmet au gestionnaire. Si vous définissez vos propres types d'entrée, c'est la seule bibliothèque dont vous avez besoin.
- com.amazonaws:aws-lambda-java-events — Types d'entrée pour les événements provenant de services qui invoquent des fonctions d'événement Lambda.
- com.amazonaws:aws-lambda-java-log4j2 – Bibliothèque Appender pour Apache Log4j 2 que vous pouvez utiliser afin d'ajouter l'ID de demande pour l'invocation en cours aux journaux de fonctions.
- AWS SDK pour Java 2.0 — Le SDK AWS officiel pour le langage de programmation Java.
- AWS SDK Lambda Durable Execution pour Java : créez des applications fiables en plusieurs étapes et des flux de travail d'intelligence artificielle qui contrôlent la progression, se rétablissent automatiquement en cas de panne et interrompent l'exécution. Pour plus d'informations, consultez la section Fonctions durables Lambda.

Ajoutez ces bibliothèques à votre définition de build comme suit :

Gradle

```
dependencies {
    implementation 'com.amazonaws:aws-lambda-java-core:1.2.2'
    implementation 'com.amazonaws:aws-lambda-java-events:3.11.1'
    runtimeOnly 'com.amazonaws:aws-lambda-java-log4j2:1.5.1'
    implementation 'software.amazon.lambda.durable:aws-durable-execution-sdk-
java:1.0.1'
}
```

Maven

```
  <dependencies>
    <dependency>
      <groupId>com.amazonaws</groupId>
      <artifactId>aws-lambda-java-core</artifactId>
      <version>1.2.2</version>
    </dependency>
    <dependency>
      <groupId>com.amazonaws</groupId>
      <artifactId>aws-lambda-java-events</artifactId>
      <version>3.11.1</version>
    </dependency>
    <dependency>
```

```
      <groupId>com.amazonaws</groupId>
      <artifactId>aws-lambda-java-log4j2</artifactId>
      <version>1.5.1</version>
    </dependency>
    <dependency>
      <groupId>software.amazon.lambda.durable</groupId>
      <artifactId>aws-durable-execution-sdk-java</artifactId>
      <version>1.0.1</version>
    </dependency>
  </dependencies>
```

> **Important**
>
> N'utilisez pas de composants privés de l'API JDK, tels que des champs privés, des méthodes ou des classes. Non-public Les composants de l'API peuvent être modifiés ou supprimés dans n'importe quelle mise à jour, ce qui peut entraîner l'interruption de votre application.

Pour plus d'informations sur la sérialisation personnalisée, consultezthe section called “Sérialisation personnalisée”.

Pour créer une fonction d'événement Java

1. Ouvrez la console Lambda.
2. Choisissez Create Event Function.
3. Configurez les paramètres suivants :
   - Nom de la fonction : saisissez le nom de la fonction.
   - Runtime : Choisissez Java 25.
4. Choisissez Create Event Function.

La console crée une fonction Lambda avec une classe de gestionnaire nommée `Hello`. Étant donné que Java est un langage compilé, vous ne pouvez pas afficher ou modifier le code source dans la console Lambda, mais vous pouvez modifier sa configuration, l’invoquer et configurer des déclencheurs.

> **Note**
>
> Pour démarrer le développement d'applications dans votre environnement local, déployez l'un des exemples d'applications disponibles dans le GitHub référentiel de ce guide.

La classe `Hello` comporte une fonction nommée `handleRequest` qui accepte un objet d'événement et un objet de contexte. Il s'agit de la fonction de gestionnaire que Lambda appelle lors de l'invocation de la fonction. Le runtime de la fonction Java obtient les événements d'invocations à partir de Lambda et les transmet au gestionnaire. Dans la configuration de fonction, la valeur de gestionnaire est `example.Hello::handleRequest`.

Pour mettre à jour le code de la fonction, vous créez un package de déploiement, qui est une archive .zip contenant le code de votre fonction. Au fur et à mesure du développement de votre fonction, nous vous conseillons de stocker le code de votre fonction dans le contrôle de code source, d'ajouter des bibliothèques et d'automatiser les déploiements. Commencez par créer un package de déploiement et mettre à jour votre code dans la ligne de commande.

Le runtime de la fonction transmet un objet de contexte au gestionnaire, en plus de l'événement d'invocation. L'objet de contexte contient des informations supplémentaires sur l'invocation, la fonction et l'environnement d'exécution. Des informations supplémentaires sont disponibles dans les variables d'environnement.

Votre fonction Lambda est fournie avec un groupe de CloudWatch journaux Logs. La fonction runtime envoie les détails de chaque appel à CloudWatch Logs. Il relaie tous les journaux que votre fonction génère pendant l'invocation. Si votre fonction renvoie une erreur, Lambda met en forme l'erreur et la renvoie à l'appelant.

Rubriques

- Définir le gestionnaire de fonctions d'événement Lambda en Java
- Déployez les fonctions d'événement Java Lambda avec des archives de fichiers .zip ou JAR
- Déployer les fonctions d'événements Java Lambda avec des images de conteneur
- Utilisation de couches pour les fonctions d'événements Java Lambda
- Personnalisation de la sérialisation pour les fonctions d'événements Lambda Java
- Personnalisation du comportement de démarrage de l'exécution Java pour les fonctions d'événement Lambda

- Utilisation de l'objet de contexte Lambda pour récupérer les informations de la fonction d'événement Java
- Enregistrez et surveillez les fonctions d'événements Java Lambda
- Instrumentation du code Java dans AWS Lambda
- Exemples d'applications Java pour AWS Lambda

Définir le gestionnaire de fonctions d'événement Lambda en Java

Le gestionnaire de fonctions d'événement Lambda est la méthode de votre code de fonction qui traite les événements. Lorsque votre fonction est invoquée, Lambda exécute la méthode du gestionnaire. Votre fonction s'exécute jusqu'à ce que le gestionnaire renvoie une réponse, se ferme ou expire.

Cette page explique comment utiliser les gestionnaires de fonctions d'événement Lambda en Java, notamment les options de configuration du projet, les conventions de dénomination et les meilleures pratiques. Cette page inclut également un exemple de fonction Lambda Java qui collecte des informations relatives à une commande, produit un reçu sous forme de fichier texte et place ce fichier dans un compartiment Amazon Simple Storage Service (Amazon S3). Pour plus d'informations sur le déploiement de votre fonction après l'avoir écrite, consultez the section called "Déploiement d'archives de fichiers .zip" ou the section called "Déploiement d'images de conteneur".

Sections

- Configuration de votre projet de gestionnaire Java
- Exemple de code de fonction d'événement Java Lambda
- Définitions de classe valides pour les gestionnaires Java
- Convention de nommage du gestionnaire
- Définition et accès à l'objet d'événement d'entrée
- Accès et utilisation de l'objet de contexte Lambda
- Utilisation de AWS SDK pour Java v2 dans votre gestionnaire
- Accès aux variables d'environnement
- Utilisation de l'état global
- Meilleures pratiques en matière de code pour les fonctions d'événement Java Lambda

Configuration de votre projet de gestionnaire Java

Lorsque vous utilisez des fonctions Lambda en Java, le processus consiste à écrire votre code, à le compiler et à déployer les artefacts compilés sur Lambda. Vous pouvez initialiser un projet Java Lambda de différentes manières. Par exemple, vous pouvez utiliser des outils tels que l'archétype Maven pour les fonctions Lambda, la commande AWS SAM CLI sam init ou même une configuration de projet Java standard dans votre IDE préféré, tel qu'IntelliJ IDEA ou Visual Studio Code. Vous pouvez également créer manuellement la structure de fichiers requise.

Un projet de fonction Lambda Java typique suit cette structure générale :

```
/project-root
    # src
        # main
            # java
                # example
                    # OrderHandler.java (contains main handler)
                    # <other_supporting_classes>
     # build.gradle OR pom.xml
```

Vous pouvez utiliser Maven ou Gradle pour créer votre projet et gérer les dépendances.

La logique de gestion principale de votre fonction réside dans un fichier Java situé sous le répertoire `src/main/java/example`. Dans l'exemple présenté sur cette page, nous nommons ce fichier `OrderHandler.java`. Outre ce fichier, vous pouvez inclure des classes Java supplémentaires selon vos besoins. Lorsque vous déployez votre fonction sur Lambda, assurez-vous de spécifier la classe Java qui contient la méthode de gestion principale que Lambda doit invoquer lors d'une invocation.

Exemple de code de fonction d'événement Java Lambda

L'exemple de code de fonction Lambda Java 21 suivant prend en compte les informations relatives à une commande, produit un reçu sous forme de fichier texte et place ce fichier dans un compartiment Amazon S3.

Example **`OrderHandler.java`**Fonction d'événement Lambda

```
package example;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import software.amazon.awssdk.core.sync.RequestBody;
import software.amazon.awssdk.services.s3.S3Client;
import software.amazon.awssdk.services.s3.model.PutObjectRequest;
import software.amazon.awssdk.services.s3.model.S3Exception;

import java.nio.charset.StandardCharsets;

/**
 * Lambda handler for processing orders and storing receipts in S3.
 */
public class OrderHandler implements RequestHandler<OrderHandler.Order, String> {
```

```
    private static final S3Client S3_CLIENT = S3Client.builder().build();

    /**
     * Record to model the input event.
     */
    public record Order(String orderId, double amount, String item) {}

    @Override
    public String handleRequest(Order event, Context context) {
        try {
            // Access environment variables
            String bucketName = System.getenv("RECEIPT_BUCKET");
            if (bucketName == null || bucketName.isEmpty()) {
                throw new IllegalArgumentException("RECEIPT_BUCKET environment variable
is not set");
            }

            // Create the receipt content and key destination
            String receiptContent = String.format("OrderID: %s\nAmount: $%.2f\nItem:
%s",
                    event.orderId(), event.amount(), event.item());
            String key = "receipts/" + event.orderId() + ".txt";

            // Upload the receipt to S3
            uploadReceiptToS3(bucketName, key, receiptContent);

            context.getLogger().log("Successfully processed order " + event.orderId() +
                    " and stored receipt in S3 bucket " + bucketName);
            return "Success";

        } catch (Exception e) {
            context.getLogger().log("Failed to process order: " + e.getMessage());
            throw new RuntimeException(e);
        }
    }

    private void uploadReceiptToS3(String bucketName, String key, String
receiptContent) {
        try {
            PutObjectRequest putObjectRequest = PutObjectRequest.builder()
                    .bucket(bucketName)
                    .key(key)
                    .build();
```

```
            // Convert the receipt content to bytes and upload to S3
            S3_CLIENT.putObject(putObjectRequest,
 RequestBody.fromBytes(receiptContent.getBytes(StandardCharsets.UTF_8)));
        } catch (S3Exception e) {
            throw new RuntimeException("Failed to upload receipt to S3: " +
 e.awsErrorDetails().errorMessage(), e);
        }
    }
}
```

Ce fichier `OrderHandler.java` comprend les sections suivantes :

- `package example` : en Java, cela peut être n'importe quoi, mais cela doit correspondre à la structure de répertoires de votre projet. Ici, nous utilisons `package example`, car la structure de répertoires est `src/main/java/example`.
- Instructions `import` : utilisez ces instructions pour importer les classes Java que votre fonction Lambda nécessite.
- `public class OrderHandler ...` : définit votre classe Java et doit être une définition de classe valide.
- `private static final S3Client S3_CLIENT ...`: Cela initialise un client S3 en dehors de l'une des méthodes de la classe. Cela oblige Lambda à exécuter ce code pendant la phase d'initialisation.
- `public record Order ...` : définissez la forme de l'événement d'entrée attendu dans cet enregistrement Java personnalisé.
- `public String handleRequest(Order event, Context context)` : il s'agit de la méthode de gestion principale, qui contient la logique principale de votre application.
- `private void uploadReceiptToS3(...) {}` : il s'agit d'une méthode auxiliaire référencée par la méthode de gestion principale `handleRequest`.

Exemples de fichiers build.gradle et pom.xml

Le fichier `build.gradle` ou `pom.xml` suivant accompagne cette fonction.

build.gradle

```
plugins {
    id 'java'
}
```

```
repositories {
    mavenCentral()
}

dependencies {
    implementation 'com.amazonaws:aws-lambda-java-core:1.2.3'
    implementation 'software.amazon.awssdk:s3:2.28.29'
    implementation 'org.slf4j:slf4j-nop:2.0.16'
}

task buildZip(type: Zip) {
    from compileJava
    from processResources
    into('lib') {
        from configurations.runtimeClasspath
    }
}

java {
    sourceCompatibility = JavaVersion.VERSION_21
    targetCompatibility = JavaVersion.VERSION_21
}

build.dependsOn buildZip
```

pom.xml

```
<project xmlns="http://maven.apache.org/POM/4.0.0" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://maven.apache.org/POM/4.0.0 http://maven.apache.org/
maven-v4_0_0.xsd">
    <modelVersion>4.0.0</modelVersion>
    <groupId>com.example</groupId>
    <artifactId>example-java</artifactId>
    <packaging>jar</packaging>
    <version>1.0-SNAPSHOT</version>
    <name>example-java-function</name>
    <properties>
        <project.build.sourceEncoding>UTF-8</project.build.sourceEncoding>
        <maven.compiler.source>21</maven.compiler.source>
        <maven.compiler.target>21</maven.compiler.target>
    </properties>
```

```
    <dependencies>
        <dependency>
            <groupId>com.amazonaws</groupId>
            <artifactId>aws-lambda-java-core</artifactId>
            <version>1.2.3</version>
        </dependency>
        <dependency>
            <groupId>software.amazon.awssdk</groupId>
            <artifactId>s3</artifactId>
            <version>2.28.29</version>
        </dependency>
        <dependency>
            <groupId>org.slf4j</groupId>
            <artifactId>slf4j-nop</artifactId>
            <version>2.0.16</version>
        </dependency>
    </dependencies>

    <build>
        <plugins>
            <plugin>
                <artifactId>maven-surefire-plugin</artifactId>
                <version>3.5.2</version>
            </plugin>
            <plugin>
                <groupId>org.apache.maven.plugins</groupId>
                <artifactId>maven-shade-plugin</artifactId>
                <version>3.4.1</version>
                <configuration>
                    <createDependencyReducedPom>false</createDependencyReducedPom>
                    <filters>
                        <filter>
                            <artifact>*:*</artifact>
                            <excludes>
                                <exclude>META-INF/*</exclude>
                                <exclude>META-INF/versions/**</exclude>
                            </excludes>
                        </filter>
                    </filters>
                </configuration>
                <executions>
                    <execution>
                        <phase>package</phase>
                        <goals>
```

```
                        <goal>shade</goal>
                    </goals>
                </execution>
            </executions>
        </plugin>
        <plugin>
            <groupId>org.apache.maven.plugins</groupId>
            <artifactId>maven-compiler-plugin</artifactId>
            <version>3.13.0</version>
            <configuration>
                <release>21</release>
            </configuration>
        </plugin>
    </plugins>
  </build>
</project>
```

Pour que cette fonction fonctionne correctement, son rôle d'exécution doit autoriser l'action `s3:PutObject`. Assurez-vous également de définir la variable d'environnement `RECEIPT_BUCKET`. Après une invocation réussie, le compartiment Amazon S3 doit contenir un fichier de reçu.

> **Note**
>
> Cette fonction peut nécessiter des paramètres de configuration supplémentaires pour s'exécuter correctement sans expiration du délai imparti. Nous recommandons de configurer 256 Mo de mémoire et un délai d'attente de 10 secondes. La première invocation peut prendre plus de temps en raison d'un démarrage à froid. Les invocations suivantes devraient s'exécuter beaucoup plus rapidement en raison de la réutilisation de l'environnement d'exécution.

Définitions de classe valides pour les gestionnaires Java

Pour définir votre classe, la bibliothèque aws-lambda-java-core définit deux interfaces pour les méthodes du gestionnaire. Utilisez les interfaces fournies pour simplifier la configuration du gestionnaire et valider la signature de la méthode au moment de la compilation.

- com.amazonaws.services.lambda.runtime. RequestHandler
- com.amazonaws.services.lambda.runtime. RequestStreamHandler

L'interface `RequestHandler` est un type générique qui prend deux paramètres : le type d'entrée et le type de sortie. Les deux types doivent être des objets. Dans cet exemple, notre classe `OrderHandler` implémente `RequestHandler<OrderHandler.Order, String>`. Le type d'entrée est l'enregistrement `Order` que nous définissons dans la classe, et le type de sortie est `String`.

```
public class OrderHandler implements RequestHandler<OrderHandler.Order, String> {
    ...
}
```

Lorsque vous utilisez cette interface, le moteur d'exécution Java désérialise l'événement dans l'objet avec le type d'entrée et sérialise la sortie en texte. Utilisez cette interface lorsque la sérialisation intégrée fonctionne avec vos types d'entrée et de sortie.

Pour utiliser votre propre sérialisation, vous pouvez implémenter l'interface `RequestStreamHandler`. Avec cette interface, Lambda transmet à votre gestionnaire un flux d'entrée et un flux de sortie. Le gestionnaire lit les octets du flux d'entrée, écrit dans le flux de sortie et renvoie une valeur vide. Pour un exemple d'utilisation de l'environnement d'exécution Java 21, consultez HandlerStream.java.

Si vous travaillez uniquement avec des types de base et génériques (c'est-à-dire `String` `IntegerList`, ou`Map`) dans votre fonction Java, vous n'avez pas besoin d'implémenter d'interface. Par exemple, si votre fonction prend une `Map<String, String>` entrée et renvoie un`String`, votre définition de classe et votre signature de gestionnaire peuvent ressembler à ce qui suit :

```
public class ExampleHandler {
    public String handleRequest(Map<String, String> input, Context context) {
        ...
    }
}
```

De plus, lorsque vous n'implémentez pas d'interface, l'objet de contexte est facultatif. Par exemple, votre définition de classe et votre signature de gestionnaire peuvent ressembler à ce qui suit :

```
public class NoContextHandler {
   public String handleRequest(Map<String, String> input) {
        ...
   }
}
```

Convention de nommage du gestionnaire

Pour les fonctions Lambda en Java, si vous implémentez l'interface `RequestHandler` ou `RequestStreamHandler`, la méthode de votre gestionnaire principal doit être nommée `handleRequest`. Incluez également la balise `@Override` au-dessus de votre méthode `handleRequest`. Lorsque vous déployez votre fonction sur Lambda, spécifiez le gestionnaire principal dans la configuration de votre fonction au format suivant :

- *<package>*. *<Class>*— Par exemple,`example.OrderHandler`.

Pour les fonctions Lambda en Java qui n'implémentent pas l'`RequestStreamHandler`interface `RequestHandler` or, vous pouvez utiliser n'importe quel nom pour le gestionnaire. Lorsque vous déployez votre fonction sur Lambda, spécifiez le gestionnaire principal dans la configuration de votre fonction au format suivant :

- *<package>*. *<Class>*: : *<handler_method_name>* — Par exemple,`example.Handler::mainHandler`.

Définition et accès à l'objet d'événement d'entrée

JSON est le format d'entrée le plus courant et standard pour les fonctions Lambda. Dans cet exemple, la fonction exige une entrée similaire à l'exemple suivant :

```
{
    "orderId": "12345",
    "amount": 199.99,
    "item": "Wireless Headphones"
}
```

Lorsque vous utilisez des fonctions Lambda dans Java 17 ou version plus récente, vous pouvez définir la forme de l'événement d'entrée attendu sous la forme d'un enregistrement Java. Dans cet exemple, nous définissons un enregistrement au sein de la classe `OrderHandler` pour représenter un objet `Order` :

```
public record Order(String orderId, double amount, String item) {}
```

Cet enregistrement correspond à la forme d'entrée attendue. Après avoir défini votre enregistrement, vous pouvez écrire une signature de gestionnaire qui utilise une entrée JSON conforme à la définition de l'enregistrement. L'environnement d'exécution Java désérialise automatiquement ce JSON en

un objet Java. Vous pouvez ensuite accéder aux champs de l'objet. Par exemple, `event.orderId` récupère la valeur de `orderId` à partir de l'entrée d'origine.

> **Note**
>
> Les enregistrements Java sont une fonctionnalité des environnements d'exécution Java 17 et des versions plus récentes uniquement. Dans toutes les exécutions Java, vous pouvez utiliser une classe pour représenter les données des événements. Dans de tels cas, vous pouvez utiliser une bibliothèque comme jackson pour désérialiser les entrées JSON.

Autres types d'événements d'entrée

Il existe de nombreux événements d'entrée possibles pour les fonctions Lambda en Java :

- `Integer`, `LongDouble`, et autres types numériques : l'événement est un nombre sans mise en forme supplémentaire, par exemple,. `3.5` Le moteur d'exécution Java convertit la valeur en un objet du type spécifié.
- `String` – L'événement est une chaîne JSON incluant des guillemets, par exemple, `"My string"`. Le moteur d'exécution convertit la valeur en objet `String`, sans guillemets.
- `List<Integer>`, `List<String>List<Object>`, et types similaires — L'événement est un tableau JSON. Le moteur d'exécution le désérialise en un objet du type ou de l'interface spécifié.
- `InputStream` – L'événement a un type JSON quelconque. Le moteur d'exécution transmet un flux d'octets du document au gestionnaire sans modification. Vous désérialisez l'entrée et écrivez la sortie dans un flux de sortie.
- Type de bibliothèque — Pour les événements envoyés par d'autres AWS services, utilisez les types de la bibliothèque aws-lambda-java-events. Par exemple, si votre fonction Lambda est invoquée par Amazon Simple Queue Service (SQS), utilisez l'objet `SQSEvent` comme entrée.

Accès et utilisation de l'objet de contexte Lambda

L'objet de contexte Lambda contient des informations sur l'invocation, la fonction et l'environnement d'exécution. Dans cet exemple, l'objet de contexte est de type `com.amazonaws.services.lambda.runtime.Context`, et constitue le deuxième argument de la fonction de gestion principale.

```
public String handleRequest(Order event, Context context) {
```

```
    ...
}
```

Si votre classe implémente l' RequestStreamHandlerinterface RequestHandlerou, l'objet de contexte est un argument obligatoire. Dans le cas contraire, l'objet de contexte est facultatif. Pour plus d'informations sur les signatures de gestionnaire acceptées valides, consultez the section called "Définitions de classe valides pour les gestionnaires Java".

Si vous appelez d'autres services à l'aide du AWS SDK, l'objet de contexte est requis dans quelques domaines clés. Par exemple, pour produire des journaux de fonctions pour Amazon CloudWatch, vous pouvez utiliser `context.getLogger()` cette méthode pour obtenir un `LambdaLogger` objet à enregistrer. Dans cet exemple, nous pouvons utiliser l'enregistreur pour enregistrer un message d'erreur si le traitement échoue pour une raison quelconque :

```
context.getLogger().log("Failed to process order: " + e.getMessage());
```

En dehors de la journalisation, vous pouvez également utiliser l'objet de contexte pour surveiller les fonctions. Pour plus d'informations sur la copie d'objets, consultez the section called "Contexte".

Utilisation de AWS SDK pour Java v2 dans votre gestionnaire

Vous utiliserez souvent les fonctions Lambda pour interagir avec d'autres AWS ressources ou pour les mettre à jour. Le moyen le plus simple d'interagir avec ces ressources est d'utiliser le AWS SDK for Java v2.

> **Note**
>
> Le AWS SDK pour Java (v1) est en mode maintenance et le support prendra fin le 31 décembre 2025. Nous vous recommandons de n'utiliser que le AWS SDK pour Java v2 à l'avenir.

Pour ajouter des dépendances du SDK à votre fonction, ajoutez-les dans votre fichier `build.gradle` pour Gradle ou dans votre fichier `pom.xml` pour Maven. Nous vous recommandons de n'ajouter que les bibliothèques dont vous avez besoin pour votre fonction. Dans l'exemple de code précédent, nous avons utilisé la bibliothèque `software.amazon.awssdk.services.s3`. Dans Gradle, vous pouvez ajouter cette dépendance en ajoutant la ligne suivante dans la section des dépendances de `build.gradle` :

```
implementation 'software.amazon.awssdk:s3:2.28.29'
```

Dans Maven, ajoutez les lignes suivantes dans la section `<dependencies>` de `pom.xml` :

```
    <dependency>
        <groupId>software.amazon.awssdk</groupId>
        <artifactId>s3</artifactId>
        <version>2.28.29</version>
    </dependency>
```

> **Note**
>
> Il ne s'agit peut-être pas de la version la plus récente du SDK. Choisissez la version du SDK adéquate pour votre application.

Importez ensuite les dépendances directement dans votre classe Java :

```
import software.amazon.awssdk.services.s3.S3Client;
import software.amazon.awssdk.services.s3.model.PutObjectRequest;
import software.amazon.awssdk.services.s3.model.S3Exception;
```

L'exemple de code initialise ensuite un client Amazon S3 comme suit :

```
private static final S3Client S3_CLIENT = S3Client.builder().build();
```

Dans cet exemple, nous avons initialisé notre client Amazon S3 en dehors de la fonction de gestionnaire principale pour éviter d'avoir à l'initialiser à chaque fois que nous invoquons notre fonction. Après avoir initialisé votre client SDK, vous pouvez l'utiliser pour interagir avec d'autres AWS services. L'exemple de code appelle l'API Amazon S3 `PutObject` comme suit :

```
PutObjectRequest putObjectRequest = PutObjectRequest.builder()
    .bucket(bucketName)
    .key(key)
    .build();

// Convert the receipt content to bytes and upload to S3
S3_CLIENT.putObject(putObjectRequest,
 RequestBody.fromBytes(receiptContent.getBytes(StandardCharsets.UTF_8)));
```

Accès aux variables d'environnement

Dans le code de votre gestionnaire, vous pouvez référencer n'importe quelle variable d'environnement à l'aide de la méthode `System.getenv()`. Dans cet exemple, nous référençons la variable d'environnement `RECEIPT_BUCKET` définie à l'aide de la ligne de code suivante :

```
String bucketName = System.getenv("RECEIPT_BUCKET");
if (bucketName == null || bucketName.isEmpty()) {
    throw new IllegalArgumentException("RECEIPT_BUCKET environment variable is not
 set");
}
```

Utilisation de l'état global

Lambda exécute votre code statique et le constructeur de classe pendant la phase d'initialisation avant d'invoquer votre fonction pour la première fois. Les ressources créées pendant l'initialisation restent en mémoire entre les invocations, ce qui vous évite d'avoir à les créer chaque fois que vous invoquez votre fonction.

Dans l'exemple de code, le code d'initialisation du client S3 se trouve en dehors de la méthode du gestionnaire principal. L'exécution initialise le client avant que la fonction n'exécute son premier événement, et le client reste disponible pour être réutilisé pendant toutes les invocations.

Meilleures pratiques en matière de code pour les fonctions d'événement Java Lambda

Respectez les directives de la liste suivante pour utiliser les pratiques exemplaires de codage lors de la création de vos fonctions Lambda :

- Séparez le gestionnaire Lambda de votre logique principale. Avec cette approche, vous pouvez créer une fonction plus testable à l'unité.
- Contrôlez les dépendances du package de déploiement de vos fonctions. L'environnement d'exécution AWS Lambda contient un certain nombre de bibliothèques. Pour activer les dernières fonctionnalités et mises à jour de sécurité, Lambda met régulièrement à jour ces bibliothèques. Ces mises à jour peuvent apporter des modifications subtiles au comportement de votre fonction Lambda. Pour disposer du contrôle total des dépendances que votre fonction utilise, empaquetez toutes vos dépendances avec votre package de déploiement.
- Réduisez la complexité de vos dépendances. Privilégiez les infrastructures plus simples qui se chargent rapidement au démarrage de l'environnement d'exécution. Par exemple, préférez les infrastructures d'injection (IoC) de dépendances Java plus simples comme Dagger ou Guice, à des plus complexes comme Spring Framework.

- Réduisez la taille de votre package de déploiement selon ses besoins d'exécution. Cela réduit le temps nécessaire au téléchargement et au déballage de votre package de déploiement avant l'invocation. Pour les fonctions créées en Java, évitez de télécharger l'intégralité de la bibliothèque du AWS SDK dans le cadre de votre package de déploiement. Dépendez plutôt de manière sélective des modules qui récupèrent les composants du SDK dont vous avez besoin (par exemple, DynamoDB, les modules du SDK Amazon S3 et les bibliothèques principales Lambda sur le site Web). GitHub

Tirez parti de la réutilisation de l'environnement d'exécution pour améliorer les performances de votre fonction. Initialisez les clients SDK et les connexions à la base de données en dehors du gestionnaire de fonctions et mettez en cache les actifs statiques localement dans le répertoire `/tmp`. Les invocations ultérieures traitées par la même instance de votre fonction peuvent réutiliser ces ressources. Cela permet d'économiser des coûts, tout en réduisant le temps d'exécution de la fonction.

Pour éviter des éventuelles fuites de données entre les invocations, n'utilisez pas l'environnement d'exécution pour stocker des données utilisateur, des événements ou d'autres informations ayant un impact sur la sécurité. Si votre fonction repose sur un état réversible qui ne peut pas être stocké en mémoire dans le gestionnaire, envisagez de créer une fonction distincte ou des versions distinctes d'une fonction pour chaque utilisateur.

Utilisez une directive keep-alive pour maintenir les connexions persistantes. Lambda purge les connexions inactives au fil du temps. Si vous tentez de réutiliser une connexion inactive lorsque vous invoquez une fonction, cela entraîne une erreur de connexion. Pour maintenir votre connexion persistante, utilisez la directive Keep-alive associée à votre environnement d'exécution. Pour un exemple, voir Réutilisation des connexions avec Keep-Alive in Node.js.

Utilisez des variables d'environnement pour transmettre des paramètres opérationnels à votre fonction. Par exemple, si vous écrivez dans un compartiment Amazon S3 au lieu de coder en dur le nom du compartiment dans lequel vous écrivez, configurez le nom du compartiment comme variable d'environnement.

Évitez d'utiliser des invocations récursives dans votre fonction Lambda, lorsque la fonction s'invoque elle-même ou démarre un processus susceptible de l'invoquer à nouveau. Cela peut entraîner un volume involontaire d'invocations de fonction et des coûts accrus. Si vous constatez un volume involontaire d'invocations, définissez immédiatement la simultanéité réservée à la fonction sur `0` afin de limiter toutes les invocations de la fonction, pendant que vous mettez à jour le code.

N'utilisez pas d'API non publiques non documentées dans le code de votre fonction Lambda. Pour les AWS Lambda environnements d'exécution gérés, Lambda applique régulièrement des mises à jour fonctionnelles et de sécurité aux API internes de Lambda. Ces mises à jour internes de l'API peuvent être incompatibles avec les versions antérieures, entraînant des conséquences imprévues telles que des échecs d'invocation si votre fonction dépend de ces API non publiques. Consultez la Référence d'API pour obtenir la liste des API accessibles au public.

Écriture du code idempotent. L'écriture de code idempotent pour vos fonctions garantit ne gestion identique des événements dupliqués. Votre code doit valider correctement les événements et gérer correctement les événements dupliqués. Pour de plus amples informations, veuillez consulterComment faire en sorte que ma fonction Lambda soit idempotente ?.

- Évitez d'utiliser le cache DNS de Java. Les fonctions Lambda mettent déjà en cache les réponses DNS. Si vous utilisez un autre cache DNS, vous risquez de subir des interruptions de connexion.

  La classe `java.util.logging.Logger` peut activer indirectement le cache DNS de la JVM. Pour remplacer les paramètres par défaut, définissez networkaddress.cache.ttl sur 0 avant de procéder à l'initialisation de `logger`. Exemple :

  ```
  public class MyHandler {
    // first set TTL property
    static{
     java.security.Security.setProperty("networkaddress.cache.ttl" , "0");
    }
   // then instantiate logger
    var logger = org.apache.logging.log4j.LogManager.getLogger(MyHandler.class);
  }
  ```

- Réduisez le temps que Lambda met à décompresser les packages de déploiement créés dans Java en plaçant vos fichiers `.jar` de dépendance dans un répertoire /lib distinct. C'est plus rapide que de placer tout le code de votre fonction dans un seul fichier jar contenant un grand nombre de `.class` fichiers. Pour obtenir des instructions, consultez Déployez les fonctions d'événement Java Lambda avec des archives de fichiers .zip ou JAR.

Déployez les fonctions d'événement Java Lambda avec des archives de fichiers .zip ou JAR

Le code de votre AWS Lambda fonction se compose de scripts ou de programmes compilés et de leurs dépendances. Pour déployer votre code de fonction vers Lambda, vous utilisez un package de déploiement. Lambda prend en charge deux types de packages de déploiement : les images conteneurs et les archives de fichiers .zip.

Cette page explique comment créer votre package de déploiement sous forme de fichier .zip ou Jar, puis utiliser le package de déploiement pour déployer votre code de fonction à AWS Lambda l'aide du AWS Command Line Interface (AWS CLI).

> **Important**
>
> Java 25 a introduit le support pour les caches Ahead-of-Time (AOT). Nous vous recommandons vivement de ne pas utiliser de caches AOT lors du déploiement de vos fonctions sous forme d'archives de fichiers .zip ou JAR, car les caches peuvent provoquer un comportement inattendu lorsque Lambda met à jour le runtime géré. Pour de plus amples informations, voirAhead-of-Time (AOT) et caches CDS.

Sections

- Conditions préalables
- Outils et bibliothèques
- Création d’un package de déploiement avec Gradle
- Utilisation des couches pour les dépendances
- Création d’un package de déploiement avec Maven
- Chargement d’un package de déploiement avec la console Lambda
- Téléchargement d'un package de déploiement à l'aide du AWS CLI
- Téléchargement d'un package de déploiement avec AWS SAM

Conditions préalables

AWS CLI Il s'agit d'un outil open source que vous pouvez utiliser pour interagir avec les AWS services à l'aide de commandes dans votre interface de ligne de commande. Pour effectuer les étapes de cette section, vous devez disposer de la version 2 de l’AWS CLI.

Outils et bibliothèques

AWS fournit les bibliothèques suivantes pour les fonctions Java. Ces bibliothèques sont disponibles via le Référentiel central Maven.

- com.amazonaws:aws-lambda-java-core (obligatoire) – Définit les interfaces de méthode du gestionnaire et l'objet contexte que l'environnement d'exécution transmet au gestionnaire. Si vous définissez vos propres types d'entrée, c'est la seule bibliothèque dont vous avez besoin.
- com.amazonaws:aws-lambda-java-events — Types d'entrée pour les événements provenant de services qui invoquent des fonctions d'événement Lambda.
- com.amazonaws:aws-lambda-java-log4j2 – Bibliothèque Appender pour Apache Log4j 2 que vous pouvez utiliser afin d'ajouter l'ID de demande pour l'invocation en cours aux journaux de fonctions.
- AWS SDK pour Java 2.0 — Le SDK AWS officiel pour le langage de programmation Java.
- AWS SDK Lambda Durable Execution pour Java : créez des applications fiables en plusieurs étapes et des flux de travail d'intelligence artificielle qui contrôlent la progression, se rétablissent automatiquement en cas de panne et interrompent l'exécution. Pour plus d'informations, consultez la section Fonctions durables Lambda.

Ajoutez ces bibliothèques à votre définition de build comme suit :

Gradle

```
dependencies {
    implementation 'com.amazonaws:aws-lambda-java-core:1.2.2'
    implementation 'com.amazonaws:aws-lambda-java-events:3.11.1'
    runtimeOnly 'com.amazonaws:aws-lambda-java-log4j2:1.5.1'
    implementation 'software.amazon.lambda.durable:aws-durable-execution-sdk-
java:1.0.1'
}
```

Maven

```
  <dependencies>
    <dependency>
      <groupId>com.amazonaws</groupId>
      <artifactId>aws-lambda-java-core</artifactId>
      <version>1.2.2</version>
    </dependency>
```

```
    <dependency>
      <groupId>com.amazonaws</groupId>
      <artifactId>aws-lambda-java-events</artifactId>
      <version>3.11.1</version>
    </dependency>
    <dependency>
      <groupId>com.amazonaws</groupId>
      <artifactId>aws-lambda-java-log4j2</artifactId>
      <version>1.5.1</version>
    </dependency>
    <dependency>
      <groupId>software.amazon.lambda.durable</groupId>
      <artifactId>aws-durable-execution-sdk-java</artifactId>
      <version>1.0.1</version>
    </dependency>
  </dependencies>
```

Afin de créer un package de déploiement, compilez votre code de fonction et vos dépendances dans un seul fichier .zip ou Java Archive (JAR). Pour Gradle, utilisez le type de build `Zip`. Pour Apache Maven, utilisez le plug-in Maven Shade. Pour télécharger votre package de déploiement, utilisez la console Lambda, l'API Lambda ou (). AWS Serverless Application Model AWS SAM

> **Note**
>
> Pour que la taille de votre package de déploiement reste petite, empaquetez les dépendances de votre fonction en couches. Les couches vous permettent de gérer vos dépendances de manière indépendante. Elles peuvent être utilisées par plusieurs fonctions et partagées avec d'autres comptes. Pour plus d'informations, consultez the section called "Layers".

Création d'un package de déploiement avec Gradle

Afin de créer un package de déploiement avec le code et les dépendances de votre fonction dans Gradle, utilisez le type de build `Zip`. Voici un exemple tiré d'un fichier exemple build.gradle complet :

Example build.gradle – Tâche de génération

```
task buildZip(type: Zip) {
    into('lib') {
```

```
        from(jar)
        from(configurations.runtimeClasspath)
    }
}
```

Cette configuration de build donne lieu à un package de déploiement dans le répertoire `build/distributions`. Dans l'instruction `into('lib')`, la tâche `jar` assemble une archive jar contenant vos classes principales dans un dossier nommé `lib`. De plus, la tâche `configurations.runtimeClassPath` copie les bibliothèques de dépendances du chemin de classe de génération dans le même dossier `lib`.

Example build.gradle – Dépendances

```
dependencies {
    ...
    implementation 'com.amazonaws:aws-lambda-java-core:1.2.2'
    implementation 'com.amazonaws:aws-lambda-java-events:3.11.1'
    implementation 'org.apache.logging.log4j:log4j-api:2.17.1'
    implementation 'org.apache.logging.log4j:log4j-core:2.17.1'
    runtimeOnly 'org.apache.logging.log4j:log4j-slf4j18-impl:2.17.1'
    runtimeOnly 'com.amazonaws:aws-lambda-java-log4j2:1.5.1'
    ...
}
```

Lambda charge les fichiers JAR dans l'ordre alphabétique Unicode. Si plusieurs fichiers JAR du répertoire `lib` contiennent la même classe, le premier fichier est utilisé. Vous pouvez utiliser le script shell suivant afin d'identifier les classes en double :

Example test-zip.sh

```
mkdir -p expanded
unzip path/to/my/function.zip -d expanded
find ./expanded/lib -name '*.jar' | xargs -n1 zipinfo -1 | grep '.*.class' | sort |
 uniq -c | sort
```

Utilisation des couches pour les dépendances

Vous pouvez empaqueter les dépendances de votre fonction par couches afin de réduire la taille de votre package de déploiement et de gérer les dépendances de manière indépendante. Pour plus d'informations, consultez the section called "Layers".

Création d'un package de déploiement avec Maven

Pour créer un package de déploiement avec Maven, utilisez le plug-in Maven Shade. Le plug-in crée un fichier JAR qui contient le code de fonction compilé et toutes ses dépendances.

Example pom.xml – Configuration du plugin

```
      <plugin>
        <groupId>org.apache.maven.plugins</groupId>
        <artifactId>maven-shade-plugin</artifactId>
        <version>3.2.2</version>
        <configuration>
          <createDependencyReducedPom>false</createDependencyReducedPom>
        </configuration>
        <executions>
          <execution>
            <phase>package</phase>
            <goals>
              <goal>shade</goal>
            </goals>
          </execution>
        </executions>
      </plugin>
```

Pour créer le package de déploiement, utilisez la commande `mvn package`.

```
[INFO] Scanning for projects...
[INFO] -----------------------< com.example:java-maven >-----------------------
[INFO] Building java-maven-function 1.0-SNAPSHOT
[INFO] --------------------------------[ jar ]---------------------------------
...
[INFO] --- maven-jar-plugin:2.4:jar (default-jar) @ java-maven ---
[INFO] Building jar: target/java-maven-1.0-SNAPSHOT.jar
[INFO]
[INFO] --- maven-shade-plugin:3.2.2:shade (default) @ java-maven ---
[INFO] Including com.amazonaws:aws-lambda-java-core:jar:1.2.2 in the shaded jar.
[INFO] Including com.amazonaws:aws-lambda-java-events:jar:3.11.1 in the shaded jar.
[INFO] Including joda-time:joda-time:jar:2.6 in the shaded jar.
[INFO] Including com.google.code.gson:gson:jar:2.8.6 in the shaded jar.
[INFO] Replacing original artifact with shaded artifact.
[INFO] Replacing target/java-maven-1.0-SNAPSHOT.jar with target/java-maven-1.0-
SNAPSHOT-shaded.jar
[INFO] ------------------------------------------------------------------------
```

```
[INFO] BUILD SUCCESS
[INFO] ------------------------------------------------------------------------
[INFO] Total time:  8.321 s
[INFO] Finished at: 2020-03-03T09:07:19Z
[INFO] ------------------------------------------------------------------------
```

Cette commande génère un fichier JAR dans le répertoire `target`.

> **Note**
>
> Si vous travaillez avec un JAR multi-version (MRJAR), vous devez inclure le MRJAR (c'est-à-dire le JAR ombré produit par le plugin Maven Shade) dans le répertoire `lib` et le zipper avant de charger votre package de déploiement sur Lambda. Sinon, Lambda risque de ne pas décompresser correctement votre fichier JAR et de l'`MANIFEST.MF`ignorer.

Si vous utilisez la bibliothèque appender (`aws-lambda-java-log4j2`), vous devez également configurer un transformateur pour le plug-in Maven Shade. La bibliothèque de transformateurs combine les versions d'un fichier cache qui apparaissent à la fois dans la bibliothèque appender et dans Log4j.

Example pom.xml – Configuration du plugin avec l'appender Log4j 2

```
      <plugin>
        <groupId>org.apache.maven.plugins</groupId>
        <artifactId>maven-shade-plugin</artifactId>
        <version>3.2.2</version>
        <configuration>
          <createDependencyReducedPom>false</createDependencyReducedPom>
        </configuration>
        <executions>
          <execution>
            <phase>package</phase>
            <goals>
              <goal>shade</goal>
            </goals>
            <configuration>
              <transformers>
                <transformer
implementation="com.github.edwgiz.maven_shade_plugin.log4j2_cache_transformer.PluginsCacheFile
                </transformer>
```

```
            </transformers>
          </configuration>
        </execution>
      </executions>
      <dependencies>
        <dependency>
          <groupId>com.github.edwgiz</groupId>
          <artifactId>maven-shade-plugin.log4j2-cachefile-transformer</artifactId>
          <version>2.13.0</version>
        </dependency>
      </dependencies>
    </plugin>
```

Chargement d’un package de déploiement avec la console Lambda

Pour créer une nouvelle fonction d'événement, vous devez d'abord créer la fonction dans la console, puis télécharger votre fichier .zip ou JAR. Pour mettre à jour une fonction existante, ouvrez la page de votre fonction, puis suivez la même procédure pour ajouter votre fichier .zip ou JAR mis à jour.

Si votre fichier package de déploiement fait moins de 50 Mo, vous pouvez créer ou mettre à jour une fonction en chargeant le fichier directement à partir de votre ordinateur local. Pour les fichiers .zip ou JAR de plus de 50 Mo, vous devez d’abord charger votre package dans un compartiment Amazon S3. Pour savoir comment charger un fichier dans un compartiment Amazon S3 à l'aide du Console de gestion AWS, consultez Getting started with Amazon S3. Pour télécharger des fichiers à l'aide de AWS CLI, voir Déplacer des objets dans le guide de AWS CLI l'utilisateur.

> **Note**
>
> Vous ne pouvez pas modifier le type de package de déploiement (.zip ou image de conteneur) d’une fonction existante. Par exemple, vous ne pouvez pas convertir une fonction d’image de conteneur pour utiliser un fichier d’archive .zip à la place. Vous devez créer une nouvelle fonction.

Pour créer une nouvelle fonction d'événement (console)

1. Ouvrez la page Event Functions de la console Lambda et choisissez Create Event Function.
2. Choisissez Créer à partir de zéro.
3. Sous Informations de base, procédez comme suit :

a. Pour Nom de la fonction, saisissez le nom de la fonction.

b. Pour Exécution, sélectionnez l'exécution que vous souhaitez utiliser.

c. (Facultatif) Pour Architecture, choisissez l'architecture de l'ensemble des instructions pour votre fonction. L'architecture par défaut est x86_64. Assurez-vous que le package de déploiement .zip pour votre fonction est compatible avec l'architecture de l'ensemble d'instructions que vous sélectionnez.

4. (Facultatif) Sous Permissions (Autorisations), développez Change default execution role (Modifier le rôle d'exécution par défaut). Vous pouvez créer un rôle d'exécution ou en utiliser un existant.
5. Choisissez Create Event Function. Lambda crée une fonction de base « Hello world » à l'aide de l'exécution de votre choix.

Pour charger une archive .zip ou JAR à partir de votre ordinateur local (console)

1. Sur la page Event Functions de la console Lambda, choisissez la fonction pour laquelle vous souhaitez télécharger le fichier .zip ou JAR.
2. Sélectionnez l'onglet Code.
3. Dans le volet Source du code, choisissez Charger à partir de.
4. Choisissez un fichier .zip ou .jar.
5. Pour charger un fichier .zip ou JAR, procédez comme suit :

   a. Sélectionnez Charger, puis choisissez votre fichier .zip ou JAR dans le sélecteur de fichiers.

   b. Choisissez Ouvrir.

   c. Cliquez sur Enregistrer.

Pour charger une archive .zip ou JAR depuis un compartiment Amazon S3 (console)

1. Sur la page Event Functions de la console Lambda, choisissez la fonction pour laquelle vous souhaitez télécharger un nouveau fichier .zip ou JAR.
2. Sélectionnez l'onglet Code.
3. Dans le volet Source du code, choisissez Charger à partir de.
4. Choisissez l'emplacement Amazon S3.
5. Collez l'URL du lien Amazon S3 de votre fichier .zip et choisissez Enregistrer.

Téléchargement d'un package de déploiement à l'aide du AWS CLI

Vous pouvez utiliser la AWS CLI pour créer une nouvelle fonction ou pour mettre à jour une fonction existante à l'aide d'un fichier .zip ou JAR. Utilisez les commandes create-function et update-function-code pour déployer votre package .zip ou JAR. Si votre fichier est inférieur à 50 Mo, vous pouvez charger le package à partir d'un emplacement de fichier sur votre machine de génération locale. Pour les fichiers plus volumineux, vous devez charger votre package .zip ou JAR à partir d'un compartiment Amazon S3. Pour savoir comment charger un fichier dans un compartiment Amazon S3 à l'aide du AWS CLI, consultez la section Déplacer des objets dans le guide de AWS CLI l'utilisateur.

> **Note**
>
> Si vous chargez votre fichier .zip ou JAR depuis un compartiment Amazon S3 à l'aide de AWS CLI, le compartiment doit se trouver dans le même emplacement Région AWS que votre fonction.

Pour créer une nouvelle fonction à l'aide d'un fichier .zip ou JAR avec le AWS CLI, vous devez spécifier les éléments suivants :

- Le nom de votre fonction (`--function-name`)
- Le runtime de votre fonction (`--runtime`)
- Le nom de ressource Amazon (ARN) du rôle d'exécution de votre fonction (`--role`)
- Le nom de la méthode du gestionnaire dans votre code de fonction (`--handler`)

Vous devez également indiquer l'emplacement de votre fichier .zip ou JAR. Si votre fichier .zip ou JAR se trouve dans un dossier sur votre machine de génération locale, utilisez l'option `--zip-file` pour spécifier le chemin d'accès du fichier, comme le montre l'exemple de commande suivant.

```
aws lambda create-function --function-name myFunction \
--runtime java25 --handler example.handler \
--role arn:aws:iam::123456789012:role/service-role/my-lambda-role \
--zip-file fileb://myFunction.zip
```

Pour spécifier l'emplacement du fichier .zip dans un compartiment Amazon S3, utilisez l'option `--code` comme le montre l'exemple de commande suivant. Vous devez uniquement utiliser le paramètre `S3ObjectVersion` pour les objets soumis à la gestion des versions.

```
aws lambda create-function --function-name myFunction \
--runtime java25 --handler example.handler \
--role arn:aws:iam::123456789012:role/service-role/my-lambda-role \
--code S3Bucket=amzn-s3-demo-
bucket,S3Key=myFileName.zip,S3ObjectVersion=myObjectVersion
```

Pour mettre à jour une fonction existante à l'aide de l'interface de ligne de commande, vous devez spécifier le nom de votre fonction à l'aide du paramètre `--function-name`. Vous devez également spécifier l'emplacement du fichier .zip que vous souhaitez utiliser pour mettre à jour votre code de fonction. Si votre fichier .zip se trouve dans un dossier sur votre machine de génération locale, utilisez l'option `--zip-file` pour spécifier le chemin d'accès du fichier, comme le montre l'exemple de commande suivant.

```
aws lambda update-function-code --function-name myFunction \
--zip-file fileb://myFunction.zip
```

Pour spécifier l'emplacement du fichier .zip dans un compartiment Amazon S3, utilisez les options `--s3-bucket` et `--s3-key` comme le montre l'exemple de commande suivant. Vous devez uniquement utiliser le paramètre `--s3-object-version` pour les objets soumis à la gestion des versions.

```
aws lambda update-function-code --function-name myFunction \
--s3-bucket amzn-s3-demo-bucket --s3-key myFileName.zip --s3-object-version myObject
 Version
```

Téléchargement d'un package de déploiement avec AWS SAM

Vous pouvez l'utiliser AWS SAM pour automatiser les déploiements de votre code de fonction, de votre configuration et de vos dépendances. AWS SAM est une extension de CloudFormation qui fournit une syntaxe simplifiée pour définir des applications sans serveur. L'exemple de modèle suivant définit une fonction avec un package de déploiement dans le répertoire `build/distributions` utilisé par Gradle :

Example template.yml

```
AWSTemplateFormatVersion: '2010-09-09'
Transform: 'AWS::Serverless-2016-10-31'
Description: An AWS Lambda application that calls the Lambda API.
Resources:
```

```
  function:
    Type: AWS::Serverless::Function
    Properties:
      CodeUri: build/distributions/java-basic.zip
      Handler: example.Handler
      Runtime: java25
      Description: Java function
      MemorySize: 512
      Timeout: 10
      # Function's execution role
      Policies:
        - AWSLambdaBasicExecutionRole
        - AWSLambda_ReadOnlyAccess
        - AWSXrayWriteOnlyAccess
        - AWSLambdaVPCAccessExecutionRole
      Tracing: Active
```

Pour créer la fonction, utilisez les commandes `package` et `deploy`. Ces commandes sont des personnalisations de l AWS CLI. Elles encapsulent d'autres commandes pour charger le package de déploiement sur Amazon S3, réécrivent le modèle avec l'URI de l'objet, et mettent à jour le code de la fonction.

L'exemple de script suivant exécute une build Gradle et télécharge le package de déploiement qu'il crée. Il crée une CloudFormation pile la première fois que vous l'exécutez. Si la pile existe déjà, le script la met à jour.

Example deploy.sh

```
#!/bin/bash
set -eo pipefail
aws cloudformation package --template-file template.yml --s3-bucket MY_BUCKET --output-
template-file out.yml
aws cloudformation deploy --template-file out.yml --stack-name java-basic --
capabilities CAPABILITY_NAMED_IAM
```

Afin d'obtenir un exemple de travail complet, consultez les exemples d'applications suivants :

Exemples d'applications Lambda en Java

- example-java — Une fonction d'événement Java qui montre comment utiliser Lambda pour traiter les commandes. Cette fonction montre comment définir et désérialiser un objet d'événement d'entrée personnalisé, utiliser le AWS SDK et enregistrer les sorties.

- java-basic – Ensemble de fonctions Java minimales avec des tests unitaires et une configuration de journalisation variable.
- java events – Ensemble de fonctions Java contenant du code squelette permettant de gérer les événements de divers services tels qu'Amazon API Gateway, Amazon SQS et Amazon Kinesis. Ces fonctions utilisent la dernière version (3.0.0 et ultérieure) de la bibliothèque aws-lambda-java-events. Ces exemples ne nécessitent pas le AWS SDK comme dépendance.
- s3-java – Fonction Java qui traite les événements de notification d'Amazon S3 et utilise la bibliothèque de classes Java (JCL) pour créer des miniatures à partir de fichiers d'image chargés.
- layer-java : fonction Java qui illustre comment utiliser une couche Lambda pour empaqueter les dépendances séparément du code de votre fonction principale.

Déployer les fonctions d'événements Java Lambda avec des images de conteneur

Il existe trois méthodes pour créer une image de conteneur pour une fonction d'événement Java Lambda :

- À l'aide d'un AWS image de base pour Java

  Les images de base AWS sont préchargées avec une exécution du langage, un client d'interface d'exécution pour gérer l'interaction entre Lambda et votre code de fonction, et un émulateur d'interface d'exécution pour les tests locaux.
- À l'aide d'un AWS OS-only image de base

  AWS OS-only les images de base contiennent une distribution Amazon Linux et l'émulateur d'interface d'exécution. Ces images sont couramment utilisées pour créer des images de conteneur pour les langages compilés, tels que Go et Rust, et pour une langue ou une version linguistique pour laquelle Lambda ne fournit pas d'image de base, telle que Node.js 19. Vous pouvez également utiliser des images OS-only de base pour implémenter un environnement d'exécution personnalisé. Pour rendre l'image compatible avec Lambda, vous devez inclure le client d'interface d'exécution pour Java dans l'image.
- Utilisation d'une image non AWS basique

  Vous pouvez utiliser une autre image de base à partir d'un autre registre de conteneur, comme Alpine Linux ou Debian. Vous pouvez également utiliser une image personnalisée créée par votre organisation. Pour rendre l'image compatible avec Lambda, vous devez inclure le client d'interface d'exécution pour Java dans l'image.

> **Tip**
>
> Pour réduire le temps nécessaire à l'activation des fonctions du conteneur Lambda, consultez Utiliser des générations en plusieurs étapes (français non garanti) dans la documentation Docker. Pour créer des images de conteneur efficaces, suivez la section Bonnes pratiques pour l'écriture de Dockerfiles (français non garanti).

Cette page explique comment créer, tester et déployer des images de conteneur pour Lambda.

Rubriques

- AWS images de base pour Java

- À l'aide d'un AWS image de base pour Java
- Utilisation d'une autre image de base avec le client d'interface d'exécution

AWS images de base pour Java

AWS fournit les images de base suivantes pour Java :

Étiquettes	Environnement d'exécution	Système d'exploitation	Dockerfile	Obsolescence
25	Java 25	Amazon Linux	Dockerfile pour Java 2.5 sur GitHub	30 juin 2029
21	Java 21	Amazon Linux	Dockerfile pour Java 21 sur GitHub	30 juin 2029
17. automne 2023	Java 17	Amazon Linux	Dockerfile pour Java 17 sur GitHub	30 juin 2029
11 juillet 2023	Java 11	Amazon Linux	Dockerfile pour Java 11 sur GitHub	30 juin 2029
8ème édition 2023	Java 8	Amazon Linux	Dockerfile pour Java 8 sur GitHub	30 juin 2029
17	Java 17	Amazon Linux 2	Dockerfile pour Java 17 sur GitHub	30 juin 2027
11	Java 11	Amazon Linux 2	Dockerfile pour Java 11 sur GitHub	30 juin 2027
8.al2	Java 8	Amazon Linux 2	Dockerfile pour Java 8 sur GitHub	30 juin 2027

Référentiel Amazon ECR : gallery.ecr. aws/lambda/java

Les images de base de Java 21 et versions ultérieures sont basées sur l'image de conteneur minimale Amazon Linux 2023. Les images de base antérieures utilisaient Amazon Linux 2. AL2023 offre plusieurs avantages par rapport à Amazon Linux2, notamment un encombrement de déploiement réduit et des versions mises à jour de bibliothèques telles que `glibc`.

AL2023-based les images utilisent `microdnf` (lié par un lien symbolique`dnf`) comme gestionnaire de packages au lieu de`yum`, qui est le gestionnaire de packages par défaut dans Amazon Linux 2. `microdnf`est une implémentation autonome de. `dnf` Pour obtenir la liste des packages inclus dans les AL2023-based images, reportez-vous aux colonnes Conteneur minimal de la section Comparaison des packages installés sur Amazon Linux 2023 Container Images. Pour plus d'informations sur les différences entre AL2023 et Amazon Linux 2, consultez Introducing the Amazon Linux 2023 runtime for AWS Lambda sur le blog AWS Compute.

> **Note**
>
> Pour exécuter AL2023-based des images localement, y compris avec AWS Serverless Application Model (AWS SAM), vous devez utiliser Docker version 20.10.10 ou ultérieure.

À l'aide d'un AWS image de base pour Java

Conditions préalables

Pour exécuter la procédure indiquée dans cette section, vous devez satisfaire aux exigences suivantes :

- Java (par exemple, Amazon Corretto)
- Apache Maven ou Gradle
- AWS CLI version 2
- Docker (version minimale 25.0.0)
- Le plug-in buildx Docker.

Création d'une image à partir d'une image de base

Maven

1. Exécutez la commande suivante pour créer un projet Maven en utilisant l'archétype de Lambda. Les paramètres suivants sont obligatoires :

   - service — Le Service AWS client à utiliser dans la fonction Lambda. Pour une liste des sources disponibles, consultez aws-sdk-java - on. v2/services GitHub
   - region — L' Région AWS endroit où vous souhaitez créer la fonction Lambda.
   - groupId : l'espace de noms complet du package de votre application.
   - artifactId : le nom de votre projet. Cette valeur devient le nom du répertoire de votre projet.

   Sous Linux et macOS, exécutez cette commande :

   ```
   mvn -B archetype:generate \
      -DarchetypeGroupId=software.amazon.awssdk \
      -DarchetypeArtifactId=archetype-lambda -Dservice=s3 -Dregion=US_WEST_2 \
      -DgroupId=com.example.myapp \
      -DartifactId=myapp
   ```

   Dans PowerShell, exécutez cette commande :

   ```
   mvn -B archetype:generate `
      "-DarchetypeGroupId=software.amazon.awssdk" `
      "-DarchetypeArtifactId=archetype-lambda" "-Dservice=s3" "-Dregion=US_WEST_2"
    `
      "-DgroupId=com.example.myapp" `
      "-DartifactId=myapp"
   ```

   L'archétype Maven pour Lambda est préconfiguré pour compiler avec Java SE 8 et inclut une dépendance au kit AWS SDK pour Java. Si vous créez votre projet avec un archétype différent ou en utilisant une autre méthode, vous devez configurer le compilateur Java pour Maven et déclarer le kit SDK comme une dépendance.

2. Ouvrez le répertoire *myapp*`/src/main/java/com/example/`*myapp* et trouvez le fichier `App.java`. Il s'agit du code de la fonction Lambda. Vous pouvez utiliser l'exemple de code fourni pour les tests ou le remplacer par le vôtre.

3. Retournez au répertoire racine du projet, puis créez un nouveau Dockerfile avec la configuration suivante :

   - Définir la propriété `FROM` sur l'URI de l'image de base.
   - Définir l'argument `CMD` pour le gestionnaire de la fonction Lambda.

   Notez que l'exemple de Dockerfile n'inclut pas d'instruction USER. Lorsque vous déployez une image de conteneur sur Lambda, Lambda définit automatiquement un utilisateur Linux par défaut disposant d'autorisations de moindre privilège. Ceci est différent du comportement standard de Docker qui est défini par défaut par l'utilisateur `root` lorsqu'aucune instruction USER n'est fournie.

   Example Dockerfile

   ```
   FROM public.ecr.aws/lambda/java:21

   # Copy function code and runtime dependencies from Maven layout
   COPY target/classes ${LAMBDA_TASK_ROOT}
   COPY target/dependency/* ${LAMBDA_TASK_ROOT}/lib/

   # Set the CMD to your handler (could also be done as a parameter override
    outside of the Dockerfile)
   CMD [ "com.example.myapp.App::handleRequest" ]
   ```

4. Compilez le projet et rassemblez les dépendances de l'environnement d'exécution.

   ```
   mvn compile dependency:copy-dependencies -DincludeScope=runtime
   ```

5. Générez l'image Docker à l'aide de la commande docker build. L'exemple suivant nomme l'image `docker-image` et lui donne la balise `test`. Pour rendre votre image compatible avec Lambda, vous devez utiliser l'option `--provenance=false`.

   ```
   docker buildx build --platform linux/amd64 --provenance=false -t docker-
   image:test .
   ```

   > **Note**
   >
   > La commande spécifie l'option `--platform linux/amd64` pour garantir la compatibilité de votre conteneur avec l'environnement d'exécution Lambda, quelle

que soit l'architecture de votre machine de génération. Si vous avez l'intention de créer une fonction Lambda à l'aide de l'architecture du jeu d'instructions ARM64, veillez à modifier la commande pour utiliser plutôt l'option `--platform linux/arm64`.

Gradle

1. Créez un répertoire pour le projet, puis passez à ce répertoire.

```
mkdir example
cd example
```

2. Exécutez la commande suivante pour que Gradle génère un nouveau projet d'application Java dans le répertoire `example` de votre environnement. Pour Sélectionner le script de construction DSL, choisissez 2 : Groovy.

```
gradle init --type java-application
```

3. Ouvrez le répertoire */example*`/app/src/main/java/`*example* et trouvez le fichier `App.java`. Il s'agit du code de la fonction Lambda. Vous pouvez utiliser l'exemple de code suivant pour le tester, ou le remplacer par le vôtre.

   Example App.java

```
package com.example;
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
public class App implements RequestHandler<Object, String> {
    public String handleRequest(Object input, Context context) {
        return "Hello world!";
    }
}
```

4. Ouvrez le fichier `build.gradle`. Si vous utilisez l'exemple de code de fonction de l'étape précédente, remplacez le contenu de `build.gradle` par ce qui suit. Si vous utilisez votre propre code de fonction, modifiez votre fichier `build.gradle` selon vos besoins.

Example build.gradle (Groovy DSL)

```
plugins {
  id 'java'
}
group 'com.example'
version '1.0-SNAPSHOT'
sourceCompatibility = 1.8
repositories {
  mavenCentral()
}
dependencies {
  implementation 'com.amazonaws:aws-lambda-java-core:1.2.1'
}
jar {
  manifest {
      attributes 'Main-Class': 'com.example.App'
  }
}
```

5. La commande `gradle init` de l'étape 2 a également généré un cas de test fictif dans le répertoire `app/test`. Pour les besoins de ce tutoriel, passez outre l'exécution des tests en supprimant le répertoire `/test`.
6. Générez le projet.

```
gradle build
```

7. Dans le répertoire racine du projet (`/example`), créez un fichier Docker avec la configuration suivante :

   - Définir la propriété `FROM` sur l'URI de l'image de base.
   - Utilisez la commande COPY pour copier le code de fonction et les dépendances d'`{LAMBDA_TASK_ROOT}`exécution dans une variable d'Lambda-defined environnement.
   - Définir l'argument `CMD` pour le gestionnaire de la fonction Lambda.

   Notez que l'exemple de Dockerfile n'inclut pas d'instruction USER. Lorsque vous déployez une image de conteneur sur Lambda, Lambda définit automatiquement un utilisateur Linux par défaut disposant d'autorisations de moindre privilège. Ceci est différent du comportement

standard de Docker qui est défini par défaut par l'utilisateur `root` lorsqu'aucune instruction USER n'est fournie.

Example Dockerfile

```
FROM public.ecr.aws/lambda/java:21

# Copy function code and runtime dependencies from Gradle layout
COPY app/build/classes/java/main ${LAMBDA_TASK_ROOT}

# Set the CMD to your handler (could also be done as a parameter override
 outside of the Dockerfile)
CMD [ "com.example.App::handleRequest" ]
```

8. Générez l'image Docker à l'aide de la commande docker build. L'exemple suivant nomme l'image `docker-image` et lui donne la balise `test`. Pour rendre votre image compatible avec Lambda, vous devez utiliser l'option `--provenance=false`.

```
docker buildx build --platform linux/amd64 --provenance=false -t docker-
image:test .
```

> **Note**
>
> La commande spécifie l'option `--platform linux/amd64` pour garantir la compatibilité de votre conteneur avec l'environnement d'exécution Lambda, quelle que soit l'architecture de votre machine de génération. Si vous avez l'intention de créer une fonction Lambda à l'aide de l'architecture du jeu d'instructions ARM64, veillez à modifier la commande pour utiliser plutôt l'option `--platform linux/arm64`.

(Facultatif) Testez l'image localement

1. Démarrez votre image Docker à l'aide de la commande docker run. Dans cet exemple, `docker-image` est le nom de l'image et `test` est la balise.

```
docker run --platform linux/amd64 -p 9000:8080 docker-image:test
```

Cette commande exécute l'image en tant que conteneur et crée un point de terminaison local à `localhost:9000/2015-03-31/functions/function/invocations`.

> **Note**
>
> Si vous avez créé l'image Docker pour l'architecture du jeu d'instructions ARM64, veillez à utiliser l'option `--platform linux/arm64` plutôt que `--platform linux/amd64`.

2. À partir d'une nouvelle fenêtre de terminal, publiez un événement au point de terminaison local.

   Linux/macOS

   Sous Linux et macOS, exécutez la commande `curl` suivante :

   ```
   curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d '{}'
   ```

   Cette commande invoque la fonction avec un événement vide et renvoie une réponse. Si vous utilisez votre propre code de fonction plutôt que l'exemple de code de fonction, vous pouvez invoquer la fonction avec une charge utile JSON. Exemple :

   ```
   curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d
    '{"payload":"hello world!"}'
   ```

   PowerShell

   Dans PowerShell, exécutez la `Invoke-WebRequest` commande suivante :

   ```
   Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/
   invocations" -Method Post -Body '{}' -ContentType "application/json"
   ```

   Cette commande invoque la fonction avec un événement vide et renvoie une réponse. Si vous utilisez votre propre code de fonction plutôt que l'exemple de code de fonction, vous pouvez invoquer la fonction avec une charge utile JSON. Exemple :

   ```
   Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/
   invocations" -Method Post -Body '{"payload":"hello world!"}' -ContentType
    "application/json"
   ```

3. Obtenez l'ID du conteneur.

```
docker ps
```

4. Utilisez la commande docker kill pour arrêter le conteneur. Dans cette commande, remplacez `3766c4ab331c` par l'ID du conteneur de l'étape précédente.

```
docker kill 3766c4ab331c
```

Déploiement de l'image

Pour charger l'image sur Amazon RIE et créer la fonction Lambda

1. Exécutez la commande get-login-password pour authentifier la CLI Docker auprès de votre registre Amazon ECR.
   - Définissez la `--region` valeur à l' Région AWS endroit où vous souhaitez créer le référentiel Amazon ECR.
   - `111122223333`Remplacez-le par votre Compte AWS identifiant.

```
aws ecr get-login-password --region us-east-1 | docker login --username AWS --
password-stdin 111122223333.dkr.ecr.us-east-1.amazonaws.com
```

2. Créez un référentiel dans Amazon ECR à l'aide de la commande create-repository.

```
aws ecr create-repository --repository-name hello-world --region us-east-1 --image-
scanning-configuration scanOnPush=true --image-tag-mutability MUTABLE
```

> **Note**
>
> Le référentiel Amazon ECR doit être Région AWS identique à la fonction Lambda.

En cas de succès, vous obtenez une réponse comme celle-ci :

```
{
    "repository": {
        "repositoryArn": "arn:aws:ecr:us-east-1:111122223333:repository/hello-
world",
```

```
        "registryId": "111122223333",
        "repositoryName": "hello-world",
        "repositoryUri": "111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-
world",
        "createdAt": "2023-03-09T10:39:01+00:00",
        "imageTagMutability": "MUTABLE",
        "imageScanningConfiguration": {
            "scanOnPush": true
        },
        "encryptionConfiguration": {
            "encryptionType": "AES256"
        }
    }
}
```

3. Copiez le `repositoryUri` à partir de la sortie de l'étape précédente.
4. Exécutez la commande docker tag pour étiqueter votre image locale dans votre référentiel Amazon ECR en tant que dernière version. Dans cette commande :

   - `docker-image:test` est le nom et la balise de votre image Docker. Il s'agit du nom et de la balise de l'image que vous avez spécifiés dans la commande `docker build`.
   - Remplacez <ECRrepositoryUri> par l'`repositoryUri` que vous avez copié. Assurez-vous d'inclure `:latest` à la fin de l'URI.

   ```
   docker tag docker-image:test <ECRrepositoryUri>:latest
   ```

   Exemple :

   ```
   docker tag docker-image:test 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-
   world:latest
   ```

5. Exécutez la commande docker push pour déployer votre image locale dans le référentiel Amazon ECR. Assurez-vous d'inclure `:latest` à la fin de l'URI du référentiel.

   ```
   docker push 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
   ```

6. Créez un rôle d'exécution pour la fonction, si vous n'en avez pas déjà un. Vous aurez besoin de l'Amazon Resource Name (ARN) du rôle à l'étape suivante.

7. Créez la fonction Lambda. Pour `ImageUri`, indiquez l'URI du référentiel mentionné précédemment. Assurez-vous d'inclure `:latest` à la fin de l'URI.

```
aws lambda create-function \
  --function-name hello-world \
  --package-type Image \
  --code ImageUri=111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \
  --role arn:aws:iam::111122223333:role/lambda-ex
```

> **Note**
>
> Vous pouvez créer une fonction en utilisant une image d'un autre AWS compte, à condition que l'image se trouve dans la même région que la fonction Lambda. Pour plus d'informations, consultez Autorisations entre comptes Amazon ECR.

8. Invoquer la fonction.

```
aws lambda invoke --function-name hello-world response.json
```

Vous devriez obtenir une réponse comme celle-ci :

```
{
  "ExecutedVersion": "$LATEST",
  "StatusCode": 200
}
```

9. Pour voir la sortie de la fonction, consultez le fichier `response.json`.

Pour mettre à jour le code de la fonction, vous devez recréer l'image, charger la nouvelle image dans le référentiel Amazon ECR, puis utiliser la commande update-function-code pour déployer l'image dans la fonction Lambda.

Lambda résout l'étiquette d'image en hachage d'image spécifique. Cela signifie que si vous pointez la balise d'image qui a été utilisée pour déployer la fonction vers une nouvelle image dans Amazon ECR, Lambda ne met pas automatiquement à jour la fonction pour utiliser la nouvelle image.

Pour déployer la nouvelle image sur la même fonction Lambda, vous devez utiliser la commande update-function-code, même si la balise d'image dans Amazon ECR reste la même. Dans l'exemple

suivant, l'option `--publish` crée une version de la fonction à l'aide de l'image du conteneur mise à jour.

```
aws lambda update-function-code \
  --function-name hello-world \
  --image-uri 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \
  --publish
```

Utilisation d'une autre image de base avec le client d'interface d'exécution

Si vous utilisez une image OS-only de base ou une image de base alternative, vous devez inclure le client d'interface d'exécution dans votre image. Le client d'interface d'exécution étend leAPI de runtime, qui gère l'interaction entre Lambda et votre code de fonction.

Installez le client d'interface d'exécution pour Java dans votre Dockerfile ou en tant que dépendance dans votre projet. Par exemple, pour installer le client d'interface d'exécution à l'aide du gestionnaire de packages Maven, ajoutez ce qui suit à votre fichier `pom.xml` :

```
<dependency>
    <groupId>com.amazonaws</groupId>
    <artifactId>aws-lambda-java-runtime-interface-client</artifactId>
    <version>2.3.2</version>
</dependency>
```

Pour plus de détails sur le package, consultez Client d'interface d'exécution AWS Lambda dans le référentiel central Maven. Vous pouvez également consulter le code source du client de l'interface d'exécution dans le GitHub référentiel AWS Lambda Java Support Libraries.

L'exemple suivant montre comment créer une image de conteneur pour Java à l'aide d'une image Amazon Corretto. Amazon Corretto est une distribution sans coût, multiplateforme et prête à la production de Open Java Development Kit (OpenJDK). Le projet Maven inclut le client d'interface d'exécution en tant que dépendance.

Conditions préalables

Pour exécuter la procédure indiquée dans cette section, vous devez satisfaire aux exigences suivantes :

- Java (par exemple, Amazon Corretto)
- Apache Maven

- AWS CLI version 2
- Docker (version minimale 25.0.0)
- Le plug-in buildx Docker.

Création d'une image à partir d'une image de base alternative

1. Créez un projet Maven. Les paramètres suivants sont obligatoires :

   - groupId : l'espace de noms complet du package de votre application.
   - artifactId : le nom de votre projet. Cette valeur devient le nom du répertoire de votre projet.

   Linux/macOS

   ```
   mvn -B archetype:generate \
      -DarchetypeArtifactId=maven-archetype-quickstart \
      -DgroupId=example \
      -DartifactId=myapp \
      -DinteractiveMode=false
   ```

   PowerShell

   ```
   mvn -B archetype:generate `
      -DarchetypeArtifactId=maven-archetype-quickstart `
      -DgroupId=example `
      -DartifactId=myapp `
      -DinteractiveMode=false
   ```

2. Ouvrez le répertoire du projet.

   ```
   cd myapp
   ```

3. Ouvrez le fichier `pom.xml` et remplacez le contenu par ce qui suit. Ce fichier inclut aws-lambda-java-runtime-interface-client en tant que dépendance. Vous pouvez également installer le client de l'interface d'exécution dans le Dockerfile. Toutefois, l'approche la plus simple consiste à inclure la bibliothèque en tant que dépendance.

   ```
   <project xmlns="http://maven.apache.org/POM/4.0.0" xmlns:xsi="http://
   www.w3.org/2001/XMLSchema-instance"
   ```

```
  xsi:schemaLocation="http://maven.apache.org/POM/4.0.0 http://maven.apache.org/
maven-v4_0_0.xsd">
  <modelVersion>4.0.0</modelVersion>
  <groupId>example</groupId>
  <artifactId>hello-lambda</artifactId>
  <packaging>jar</packaging>
  <version>1.0-SNAPSHOT</version>
  <name>hello-lambda</name>
  <url>http://maven.apache.org</url>
  <properties>
    <maven.compiler.source>1.8</maven.compiler.source>
    <maven.compiler.target>1.8</maven.compiler.target>
  </properties>
  <dependencies>
    <dependency>
      <groupId>com.amazonaws</groupId>
      <artifactId>aws-lambda-java-runtime-interface-client</artifactId>
      <version>2.3.2</version>
    </dependency>
  </dependencies>
  <build>
    <plugins>
      <plugin>
        <groupId>org.apache.maven.plugins</groupId>
        <artifactId>maven-dependency-plugin</artifactId>
        <version>3.1.2</version>
        <executions>
          <execution>
            <id>copy-dependencies</id>
            <phase>package</phase>
            <goals>
              <goal>copy-dependencies</goal>
            </goals>
          </execution>
        </executions>
      </plugin>
    </plugins>
  </build>
</project>
```

4. Ouvrez le répertoire *myapp*`/src/main/java/com/example/`*myapp* et trouvez le fichier `App.java`. Il s'agit du code de la fonction Lambda. Remplacez le code par ce qui suit.

Example gestionnaire de fonctions

```
package example;

public class App {
    public static String sayHello() {
        return "Hello world!";
    }
}
```

5. La commande `mvn -B archetype:generate` de l'étape 1 a également généré un cas de test fictif dans le répertoire `src/test`. Pour les besoins de ce tutoriel, passez outre l'exécution des tests en supprimant l'intégralité de ce répertoire `/test` généré.
6. Retournez au répertoire racine du projet, puis créez un nouveau Dockerfile. L'exemple de Dockerfile suivant utilise une image Amazon Corretto. Amazon Corretto est une distribution sans coût, multiplateforme et prête à la production d'OpenJDK.

   - Définissez la propriété `FROM` sur l'URI de l'image de base.
   - Définissez le `ENTRYPOINT` sur le module que vous souhaitez que le conteneur Docker exécute lorsqu'il démarre. Dans ce cas, le module est le client d'interface d'exécution.
   - Définir l'argument `CMD` pour le gestionnaire de la fonction Lambda.

   Notez que l'exemple de Dockerfile n'inclut pas d'instruction USER. Lorsque vous déployez une image de conteneur sur Lambda, Lambda définit automatiquement un utilisateur Linux par défaut disposant d'autorisations de moindre privilège. Ceci est différent du comportement standard de Docker qui est défini par défaut par l'utilisateur `root` lorsqu'aucune instruction `USER` n'est fournie.

   Example Dockerfile

```
FROM public.ecr.aws/amazoncorretto/amazoncorretto:21 as base

# Configure the build environment
FROM base as build
RUN yum install -y maven
WORKDIR /src

# Cache and copy dependencies
```

```
ADD pom.xml .
RUN mvn dependency:go-offline dependency:copy-dependencies

# Compile the function
ADD . .
RUN mvn package

# Copy the function artifact and dependencies onto a clean base
FROM base
WORKDIR /function

COPY --from=build /src/target/dependency/*.jar ./
COPY --from=build /src/target/*.jar ./

# Set runtime interface client as default command for the container runtime
ENTRYPOINT [ "/usr/bin/java", "-cp", "./*",
 "com.amazonaws.services.lambda.runtime.api.client.AWSLambda" ]
# Pass the name of the function handler as an argument to the runtime
CMD [ "example.App::sayHello" ]
```

7. Générez l'image Docker à l'aide de la commande docker build. L'exemple suivant nomme l'image `docker-image` et lui donne la balise `test`. Pour rendre votre image compatible avec Lambda, vous devez utiliser l'option `--provenance=false`.

```
docker buildx build --platform linux/amd64 --provenance=false -t docker-image:test
 .
```

> **Note**
>
> La commande spécifie l'option `--platform linux/amd64` pour garantir la compatibilité de votre conteneur avec l'environnement d'exécution Lambda, quelle que soit l'architecture de votre machine de génération. Si vous avez l'intention de créer une fonction Lambda à l'aide de l'architecture du jeu d'instructions ARM64, veillez à modifier la commande pour utiliser plutôt l'option `--platform linux/arm64`.

(Facultatif) Testez l'image localement

Utilisez l'émulateur d'interface d'exécution pour tester l'image localement. Vous pouvez intégrer l'émulateur dans votre image ou utiliser la procédure suivante pour l'installer sur votre machine locale.

Pour installer et exécuter l'émulateur d'interface d'exécution sur votre ordinateur local

1. Depuis le répertoire de votre projet, exécutez la commande suivante pour télécharger l'émulateur d'interface d'exécution (architecture x86-64) GitHub et l'installer sur votre machine locale.

   Linux/macOS

   ```
   mkdir -p ~/.aws-lambda-rie && \
       curl -Lo ~/.aws-lambda-rie/aws-lambda-rie https://github.com/aws/aws-lambda-runtime-interface-emulator/releases/latest/download/aws-lambda-rie && \
       chmod +x ~/.aws-lambda-rie/aws-lambda-rie
   ```

   Pour installer l'émulateur arm64, remplacez l'URL du GitHub référentiel dans la commande précédente par la suivante :

   ```
   https://github.com/aws/aws-lambda-runtime-interface-emulator/releases/latest/download/aws-lambda-rie-arm64
   ```

   PowerShell

   ```
   $dirPath = "$HOME\.aws-lambda-rie"
   if (-not (Test-Path $dirPath)) {
       New-Item -Path $dirPath -ItemType Directory
   }

   $downloadLink = "https://github.com/aws/aws-lambda-runtime-interface-emulator/releases/latest/download/aws-lambda-rie"
   $destinationPath = "$HOME\.aws-lambda-rie\aws-lambda-rie"
   Invoke-WebRequest -Uri $downloadLink -OutFile $destinationPath
   ```

   Pour installer l'émulateur arm64, remplacez `$downloadLink` par ce qui suit :

   ```
   https://github.com/aws/aws-lambda-runtime-interface-emulator/releases/latest/download/aws-lambda-rie-arm64
   ```

2. Démarrez votre image Docker à l'aide de la commande docker run. Notez ce qui suit :

   - `docker-image` est le nom de l'image et `test` est la balise.

- `/usr/bin/java -cp './*' com.amazonaws.services.lambda.runtime.api.client.AWSLambda example.App::sayHello` est le `ENTRYPOINT` suivi du `CMD` depuis votre Dockerfile.

Linux/macOS

```
docker run --platform linux/amd64 -d -v ~/.aws-lambda-rie:/aws-lambda -p
 9000:8080 \
    --entrypoint /aws-lambda/aws-lambda-rie \
    docker-image:test \
        /usr/bin/java -cp './*'
 com.amazonaws.services.lambda.runtime.api.client.AWSLambda
 example.App::sayHello
```

PowerShell

```
docker run --platform linux/amd64 -d -v "$HOME\.aws-lambda-rie:/aws-lambda" -p
 9000:8080 `
--entrypoint /aws-lambda/aws-lambda-rie `
docker-image:test `
    /usr/bin/java -cp './*'
 com.amazonaws.services.lambda.runtime.api.client.AWSLambda
 example.App::sayHello
```

Cette commande exécute l'image en tant que conteneur et crée un point de terminaison local à `localhost:9000/2015-03-31/functions/function/invocations`.

> **Note**
>
> Si vous avez créé l'image Docker pour l'architecture du jeu d'instructions ARM64, veillez à utiliser l'option `--platform linux/arm64` plutôt que `--platform linux/amd64`.

3. Publiez un événement au point de terminaison local.

Linux/macOS

Sous Linux et macOS, exécutez la commande `curl` suivante :

```
curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d '{}'
```

Cette commande invoque la fonction avec un événement vide et renvoie une réponse. Si vous utilisez votre propre code de fonction plutôt que l'exemple de code de fonction, vous pouvez invoquer la fonction avec une charge utile JSON. Exemple :

```
curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d
 '{"payload":"hello world!"}'
```

PowerShell

Dans PowerShell, exécutez la `Invoke-WebRequest` commande suivante :

```
Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/
invocations" -Method Post -Body '{}' -ContentType "application/json"
```

Cette commande invoque la fonction avec un événement vide et renvoie une réponse. Si vous utilisez votre propre code de fonction plutôt que l'exemple de code de fonction, vous pouvez invoquer la fonction avec une charge utile JSON. Exemple :

```
Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/
invocations" -Method Post -Body '{"payload":"hello world!"}' -ContentType
 "application/json"
```

4. Obtenez l'ID du conteneur.

```
docker ps
```

5. Utilisez la commande docker kill pour arrêter le conteneur. Dans cette commande, remplacez `3766c4ab331c` par l'ID du conteneur de l'étape précédente.

```
docker kill 3766c4ab331c
```

Déploiement de l'image

Pour charger l'image sur Amazon RIE et créer la fonction Lambda

1. Exécutez la commande get-login-password pour authentifier la CLI Docker auprès de votre registre Amazon ECR.

   - Définissez la `--region` valeur à l' Région AWS endroit où vous souhaitez créer le référentiel Amazon ECR.
   - `111122223333`Remplacez-le par votre Compte AWS identifiant.

   ```
   aws ecr get-login-password --region us-east-1 | docker login --username AWS --
   password-stdin 111122223333.dkr.ecr.us-east-1.amazonaws.com
   ```

2. Créez un référentiel dans Amazon ECR à l'aide de la commande create-repository.

   ```
   aws ecr create-repository --repository-name hello-world --region us-east-1 --image-
   scanning-configuration scanOnPush=true --image-tag-mutability MUTABLE
   ```

   > **Note**
   >
   > Le référentiel Amazon ECR doit être Région AWS identique à la fonction Lambda.

   En cas de succès, vous obtenez une réponse comme celle-ci :

   ```
   {
       "repository": {
           "repositoryArn": "arn:aws:ecr:us-east-1:111122223333:repository/hello-
   world",
           "registryId": "111122223333",
           "repositoryName": "hello-world",
           "repositoryUri": "111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-
   world",
           "createdAt": "2023-03-09T10:39:01+00:00",
           "imageTagMutability": "MUTABLE",
           "imageScanningConfiguration": {
               "scanOnPush": true
           },
           "encryptionConfiguration": {
   ```

```
            "encryptionType": "AES256"
        }
    }
}
```

3. Copiez le `repositoryUri` à partir de la sortie de l'étape précédente.
4. Exécutez la commande docker tag pour étiqueter votre image locale dans votre référentiel Amazon ECR en tant que dernière version. Dans cette commande :
   - `docker-image:test` est le nom et la balise de votre image Docker. Il s'agit du nom et de la balise de l'image que vous avez spécifiés dans la commande `docker build`.
   - Remplacez <ECRrepositoryUri> par l'`repositoryUri` que vous avez copié. Assurez-vous d'inclure `:latest` à la fin de l'URI.

   ```
   docker tag docker-image:test <ECRrepositoryUri>:latest
   ```

   Exemple :

   ```
   docker tag docker-image:test 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
   ```
5. Exécutez la commande docker push pour déployer votre image locale dans le référentiel Amazon ECR. Assurez-vous d'inclure `:latest` à la fin de l'URI du référentiel.

   ```
   docker push 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
   ```
6. Créez un rôle d'exécution pour la fonction, si vous n'en avez pas déjà un. Vous aurez besoin de l'Amazon Resource Name (ARN) du rôle à l'étape suivante.
7. Créez la fonction Lambda. Pour `ImageUri`, indiquez l'URI du référentiel mentionné précédemment. Assurez-vous d'inclure `:latest` à la fin de l'URI.

   ```
   aws lambda create-function \
     --function-name hello-world \
     --package-type Image \
     --code ImageUri=111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \
     --role arn:aws:iam::111122223333:role/lambda-ex
   ```

> **Note**
>
> Vous pouvez créer une fonction en utilisant une image d'un autre AWS compte, à condition que l'image se trouve dans la même région que la fonction Lambda. Pour plus d'informations, consultez Autorisations entre comptes Amazon ECR.

8. Invoquer la fonction.

```
aws lambda invoke --function-name hello-world response.json
```

Vous devriez obtenir une réponse comme celle-ci :

```
{
  "ExecutedVersion": "$LATEST",
  "StatusCode": 200
}
```

9. Pour voir la sortie de la fonction, consultez le fichier `response.json`.

Pour mettre à jour le code de la fonction, vous devez recréer l'image, charger la nouvelle image dans le référentiel Amazon ECR, puis utiliser la commande update-function-code pour déployer l'image dans la fonction Lambda.

Lambda résout l'étiquette d'image en hachage d'image spécifique. Cela signifie que si vous pointez la balise d'image qui a été utilisée pour déployer la fonction vers une nouvelle image dans Amazon ECR, Lambda ne met pas automatiquement à jour la fonction pour utiliser la nouvelle image.

Pour déployer la nouvelle image sur la même fonction Lambda, vous devez utiliser la commande update-function-code, même si la balise d'image dans Amazon ECR reste la même. Dans l'exemple suivant, l'option `--publish` crée une version de la fonction à l'aide de l'image du conteneur mise à jour.

```
aws lambda update-function-code \
  --function-name hello-world \
  --image-uri 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \
  --publish
```

Utilisation de couches pour les fonctions d'événements Java Lambda

Utilisez les couches Lambda pour empaqueter le code et les dépendances que vous souhaitez réutiliser dans plusieurs fonctions. Les couches contiennent généralement des dépendances de bibliothèque, une exécution personnalisée, ou des fichiers de configuration. La création d'une couche implique trois étapes générales :

1. Empaquetez le contenu de votre couche. Cela signifie créer une archive de fichiers .zip contenant les dépendances que vous souhaitez utiliser dans vos fonctions.
2. Créez la couche dans Lambda.
3. Ajoutez la couche à vos fonctions.

Rubriques

- Empaqueter le contenu de votre couche
- Créer la couche dans Lambda
- Ajouter la couche à votre fonction

Empaqueter le contenu de votre couche

Pour créer une couche, regroupez vos packages dans une archive (fichier .zip) répondant aux exigences suivantes :

- Assurez-vous que la version Java à laquelle Maven ou Gradle fait référence est identique à la version Java de la fonction que vous souhaitez déployer. Par exemple, pour une fonction Java 25, la `mvn -v` commande doit répertorier Java 25 dans la sortie.
- Vos dépendances doivent être stockées dans le répertoire `java/lib`, à la racine du fichier .zip. Pour plus d'informations, consultez Chemins d'accès de couche pour chaque exécution Lambda.
- Les packages de votre couche doivent être compatibles avec Linux. Les fonctions Lambda s'exécutent sur Amazon Linux.

Vous pouvez créer des couches contenant des bibliothèques Java tierces ou vos propres modules et packages Java. La procédure suivante utilise Maven. Vous pouvez également utiliser Gradle pour empaqueter le contenu de votre couche.

Créer une couche à l'aide de dépendances Maven

1. Créez un projet Apache Maven avec un fichier `pom.xml` qui définit vos dépendances.

   L'exemple suivant inclut Jackson Databind pour le traitement JSON. La section `<build>` utilise le plug-in maven-dependency-plugin pour créer des fichiers JAR distincts pour chaque dépendance au lieu de les regrouper dans un seul fichier uber-jar. Si vous souhaitez créer un fichier uber-jar, utilisez le plug-in maven-shade-plugin.

   Example pom.xml

```
<dependencies>
    <dependency>
        <groupId>com.fasterxml.jackson.core</groupId>
        <artifactId>jackson-databind</artifactId>
        <version>2.17.0</version>
    </dependency>
</dependencies>

<build>
    <plugins>
        <plugin>
            <groupId>org.apache.maven.plugins</groupId>
            <artifactId>maven-compiler-plugin</artifactId>
            <version>3.13.0</version>
            <configuration>
                <source>21</source>
                <target>21</target>
                <release>21</release>
            </configuration>
        </plugin>

        <plugin>
            <groupId>org.apache.maven.plugins</groupId>
            <artifactId>maven-dependency-plugin</artifactId>
            <version>3.6.1</version>
            <executions>
                <execution>
                    <id>copy-dependencies</id>
                    <phase>package</phase>
                    <goals>
                        <goal>copy-dependencies</goal>
                    </goals>
```

```
                    <configuration>
                        <outputDirectory>${project.build.directory}/lib</
outputDirectory>
                    </configuration>
                </execution>
            </executions>
        </plugin>
    </plugins>
</build>
```

2. Générez le projet. Cette commande crée tous les fichiers JAR de dépendance dans le répertoire `target/lib/`.

```
mvn clean package
```

3. Créez la structure de répertoires requise pour votre couche :

```
mkdir -p java/lib
```

4. Copiez les fichiers JAR de dépendance dans le répertoire `java/lib` :

```
cp target/lib/*.jar java/lib/
```

5. Compressez le contenu de la couche :

   Linux/macOS

   ```
   zip -r layer.zip java/
   ```

   PowerShell

   ```
   Compress-Archive -Path .\java -DestinationPath .\layer.zip
   ```

   La structure de répertoire de votre fichier .zip devrait se présenter comme suit :

```
java/
### lib/
    ### jackson-databind-2.17.0.jar
    ### jackson-core-2.17.0.jar
    ### jackson-annotations-2.17.0.jar
```

> **Note**
>
> Assurez-vous que votre fichier .zip inclut le répertoire `java` au niveau racine avec `lib` à l'intérieur. Cette structure garantit que Lambda peut localiser et importer vos bibliothèques. Chaque dépendance est conservée dans un fichier JAR distinct plutôt que regroupée dans un fichier uber-jar.

Créer la couche dans Lambda

Vous pouvez publier votre couche à l'aide de la console Lambda AWS CLI ou de la console Lambda.

AWS CLI

Exécutez la AWS CLI commande publish-layer-version pour créer la couche Lambda :

```
aws lambda publish-layer-version --layer-name my-layer --zip-file fileb://layer.zip
 --compatible-runtimes java25
```

Le paramètre compatible runtimes est facultatif. Lorsqu'il est spécifié, Lambda utilise ce paramètre pour filtrer les couches dans la console Lambda.

Console

Pour créer une couche (console)

1. Ouvrez la page Couches de la console Lambda.
2. Sélectionnez Créer un calque.
3. Choisissez Charger un fichier .zip, puis chargez l'archive .zip que vous avez créée précédemment.
4. (Facultatif) Pour Environnements d'exécution compatibles, choisissez l'environnement d'exécution Java qui correspond à la version de Java que vous avez utilisée pour créer votre couche.
5. Cliquez sur Créer.

Ajouter la couche à votre fonction

AWS CLI

Pour associer la couche à votre fonction, exécutez la commande update-function-configuration AWS CLI . Utilisez l'ARN de la couche pour le paramètre `--layers`. L'ARN doit spécifier la version (par exemple, `arn:aws:lambda:us-east-1:123456789012:layer:my-layer:1`). Pour plus d'informations, consultez Couches et versions de couches.

```
aws lambda update-function-configuration --function-name my-function --cli-binary-format raw-in-base64-out --layers "arn:aws:lambda:us-east-1:123456789012:layer:my-layer:1"
```

L'cli-binary-formatoption est obligatoire si vous utilisez AWS CLI la version 2. Pour faire de ce paramètre le paramètre par défaut, exécutez `aws configure set cli-binary-format raw-in-base64-out`. Pour plus d'informations, consultez les options de ligne de commande globales AWS CLI prises en charge dans le Guide de l'utilisateur AWS Command Line Interface version 2.

Console

Ajouter une couche à une fonction

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez la fonction.
3. Faites défiler jusqu'à la section Couches, puis choisissez Ajouter une couche.
4. Sous Choisir une couche, sélectionnez Couches personnalisées, puis choisissez votre couche.

   > **Note**
   >
   > Si vous n'avez pas ajouté d'environnement d'exécution compatible lors de la création de la couche, celle-ci ne sera pas répertoriée ici. Vous pouvez spécifier l'ARN de la couche à la place.

5. Choisissez Ajouter.

Personnalisation de la sérialisation pour les fonctions d'événements Lambda Java

Les environnements d’exécution gérés par Lambda Java prennent en charge la sérialisation personnalisée pour les événements JSON. La sérialisation personnalisée peut simplifier votre code et potentiellement améliorer les performances.

Rubriques

- Cas d’utilisation de la sérialisation personnalisée
- Implémentation de sérialisation personnalisée
- Test de la sérialisation personnalisée

Cas d’utilisation de la sérialisation personnalisée

Lorsque votre fonction Lambda est invoquée, les données d’événement d’entrée doivent être désérialisées dans un objet Java, et la sortie de votre fonction doit être sérialisée à nouveau dans un format pouvant être renvoyé en tant que réponse de la fonction. Les environnements d'exécution gérés par Lambda Java fournissent des fonctionnalités de sérialisation et de désérialisation par défaut qui fonctionnent bien pour gérer les charges utiles d'événements provenant de divers services, AWS tels qu'Amazon API Gateway et Amazon Simple Queue Service (Amazon SQS). Pour utiliser ces événements d’intégration de services dans votre fonction, ajoutez la dépendance aws-java-lambda-events à votre projet. Cette AWS bibliothèque contient des objets Java représentant ces événements d'intégration de services.

Vous pouvez également utiliser vos propres objets pour représenter l’événement JSON que vous transmettez à votre fonction Lambda. L’environnement d’exécution géré tente de sérialiser le JSON vers une nouvelle instance de votre objet avec son comportement par défaut. Si le sérialiseur par défaut n'a pas le comportement souhaité pour votre cas d'utilisation, utilisez la sérialisation personnalisée.

Par exemple, si votre gestionnaire de fonctions attend une classe `Vehicle` en entrée, avec la structure suivante :

```
public class Vehicle {
    private String vehicleType;
    private long vehicleId;
}
```

Cependant, les données utiles de l’événement JSON ressemblent à ceci :

```
{
    "vehicle-type": "car",
    "vehicleID": 123
}
```

Dans ce scénario, la sérialisation par défaut dans l'environnement d'exécution géré s'attend à ce que les noms de propriété JSON correspondent au camel case des noms de propriété de classe Java (`vehicleType`, `vehicleId`). Dans la mesure où les noms des propriétés dans l'événement JSON ne sont pas écrits en camel case (`vehicle-type`,`vehicleID`), vous devez utiliser une sérialisation personnalisée.

Implémentation de sérialisation personnalisée

Utilisez une interface de fournisseur de services pour charger le sérialiseur de votre choix au lieu de la logique de sérialisation par défaut du runtime géré. Vous pouvez sérialiser vos données utiles d'événements JSON directement dans des objets Java, à l'aide de l'interface standard `RequestHandler`.

Pour utiliser la sérialisation personnalisée dans votre fonction d'événement Java Lambda

1. Ajoutez la bibliothèque aws-lambda-java-core en tant que dépendance. Cette bibliothèque inclut l'CustomPojoSerializerinterface, ainsi que d'autres définitions d'interface permettant de travailler avec Java dans Lambda.
2. Créez un fichier nommé `com.amazonaws.services.lambda.runtime.CustomPojoSerializer` dans votre répertoire `src/main/resources/META-INF/services/` de votre projet.
3. Dans ce fichier, spécifiez le nom complet de votre implémentation de sérialiseur personnalisé, qui doit implémenter l'interface `CustomPojoSerializer`. Exemple :

   ```
   com.mycompany.vehicles.CustomLambdaSerialzer
   ```
4. Implémentez l'interface `CustomPojoSerializer` pour fournir votre logique de sérialisation personnalisée.
5. Utilisez l'interface standard `RequestHandler` de votre fonction Lambda. L'environnement d'exécution géré utilisera votre sérialiseur personnalisé.

Pour plus d'exemples de mise en œuvre de la sérialisation personnalisée à l'aide de bibliothèques populaires telles que FastJSON, Gson, Moshi et jackson-jr, consultez l'exemple de sérialisation personnalisée dans le référentiel. AWS GitHub

Test de la sérialisation personnalisée

Testez votre fonction pour vous assurer que votre logique de sérialisation et de désérialisation fonctionne comme prévu. Vous pouvez utiliser l'interface de ligne de AWS Serverless Application Model commande (AWS SAMCLI) pour émuler l'invocation de votre charge utile Lambda. Cela peut vous aider à tester et à itérer rapidement votre fonction lorsque vous introduisez un sérialiseur personnalisé.

1. Créez un fichier avec la charge utile de l'événement JSON avec laquelle vous souhaitez appeler votre fonction, puis appelez le AWS SAMCLI.
2. Exécutez la commande sam local invoke pour invoquer votre fonction localement. Exemple :

```
sam local invoke -e src/test/resources/event.json
```

Pour plus d'informations, voir Invoquer localement des fonctions Lambda avec. AWS SAM

Personnalisation du comportement de démarrage de l'exécution Java pour les fonctions d'événement Lambda

Cette page décrit les paramètres spécifiques aux fonctions événementielles Java dans AWS Lambda. Vous pouvez utiliser ces paramètres pour personnaliser le comportement de démarrage de l'exécution Java. Cela permet de réduire le temps de latence et d'améliorer les performances globales de la fonction, sans avoir à modifier le code.

Sections

- Comprendre la variable d'environnement JAVA_TOOL_OPTIONS
- Patch Log4j pour Log4Shell
- Ahead-of-Time (AOT) et caches CDS

Comprendre la variable d'environnement **`JAVA_TOOL_OPTIONS`**

Sur Java, Lambda prend en charge la variable d'environnement `JAVA_TOOL_OPTIONS` pour définir des variables de ligne de commande supplémentaires dans Lambda. Vous pouvez utiliser cette variable d'environnement de différentes manières, par exemple pour personnaliser les paramètres de compilation par niveaux. L'exemple suivant montre comment utiliser la variable d'environnement `JAVA_TOOL_OPTIONS` pour ce cas d'utilisation.

Exemple : personnalisation des paramètres de compilation par niveaux

La compilation par niveaux est une fonctionnalité de la JVM (Java Virtual Machine). Vous pouvez utiliser des paramètres de compilation par niveaux spécifiques pour tirer le meilleur parti des compilateurs juste à temps (JIT) de la JVM. Généralement, le compilateur C1 est optimisé pour un démarrage rapide. Le compilateur C2 est optimisé pour obtenir les meilleures performances globales, mais il utilise également plus de mémoire et prend plus de temps pour y parvenir.

Il existe cinq niveaux différents de compilation par niveaux. Au niveau 0, la JVM interprète le bytecode Java. Au niveau 4, la JVM utilise le compilateur C2 pour analyser les données de profilage collectées lors du démarrage de l'application. Au fil du temps, elle surveille l'utilisation du code pour identifier les meilleures optimisations.

La personnalisation du niveau de compilation à plusieurs niveaux peut vous aider à optimiser les performances de vos fonctions Java. Pour les petites fonctions qui s'exécutent rapidement, le réglage de la compilation hiérarchisée au niveau 1 peut contribuer à améliorer les performances de démarrage à froid en faisant en sorte que la JVM utilise le compilateur C1. Ce paramètre produit

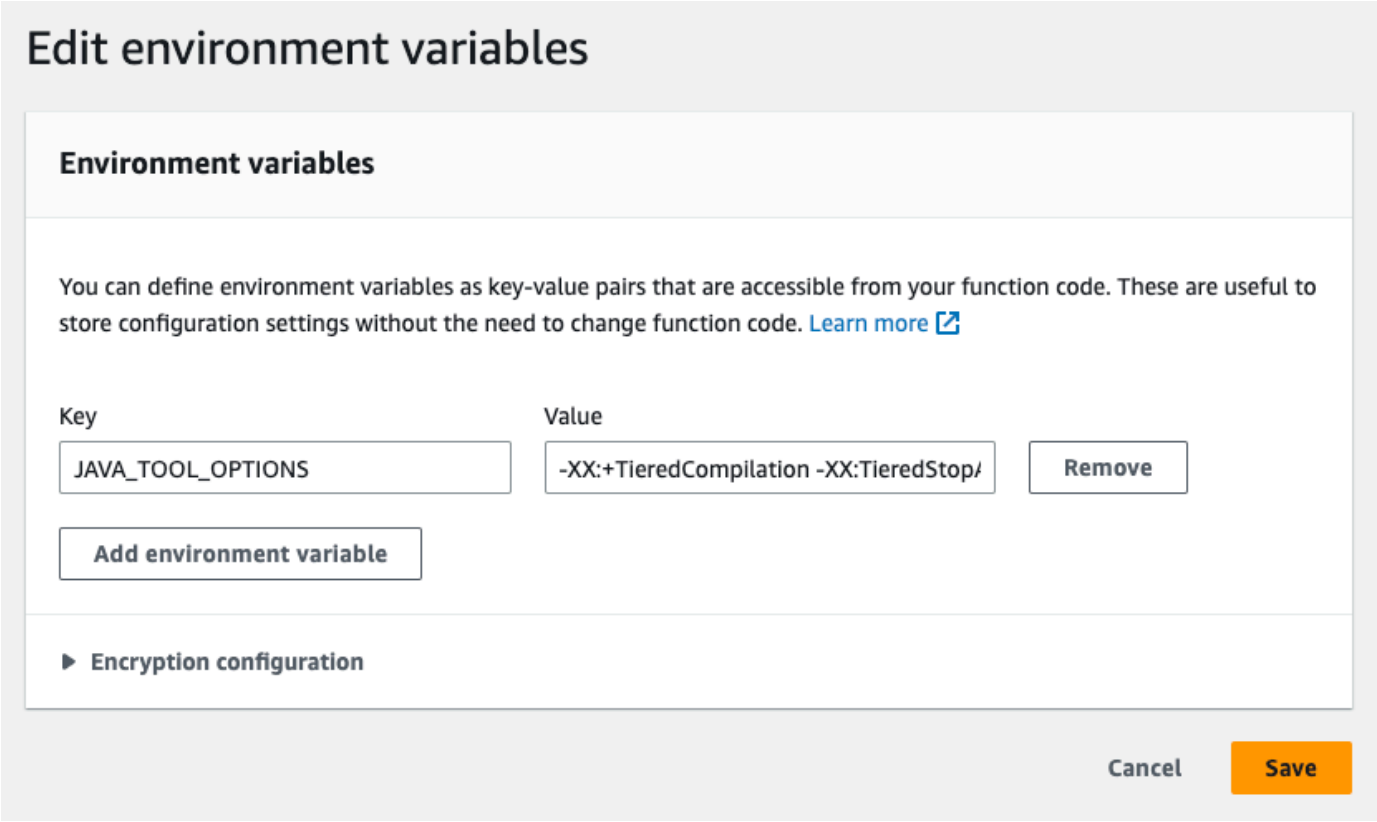
rapidement du code natif optimisé, mais il ne génère aucune donnée de profilage et n'utilise jamais le compilateur C2. Pour les fonctions plus volumineuses nécessitant des calculs intensifs, le fait de définir la compilation hiérarchisée au niveau 4 maximise les performances globales au détriment d'une consommation de mémoire supplémentaire et d'un travail d'optimisation supplémentaire lors des premiers appels après le provisionnement de chaque environnement d'exécution Lambda.

Pour les environnements d'exécution Java 11 et inférieurs, Lambda utilise les paramètres de compilation hiérarchisée par défaut de la JVM. Pour Java 17 et Java 21, Lambda configure la JVM pour arrêter la compilation hiérarchisée au niveau 1 par défaut. À partir de Java 25, Lambda arrête toujours la compilation hiérarchisée au niveau 1 par défaut, sauf en cas d'utilisation SnapStart ou de provisionnement de la concurrence, auquel cas les paramètres JVM par défaut sont utilisés.

Cela améliore les performances SnapStart et la simultanéité provisionnée sans entraîner de pénalité de démarrage à froid, car la compilation à plusieurs niveaux est effectuée en dehors du chemin d'appel dans ces cas. Pour optimiser cet avantage, vous pouvez utiliser l'amorçage, c'est-à-dire l'exécution de chemins de code lors de l'initialisation de la fonction pour déclencher le JIT avant de prendre le SnapStart snapshot ou lorsque les environnements d'exécution de la concurrence provisionnée sont préprovisionnés. Pour plus d'informations, consultez le billet de blog Optimisation des performances de démarrage à froid de AWS Lambda à l'aide de stratégies d'amorçage avancées avec. SnapStart

Pour personnaliser les paramètres de compilation par niveaux (console)

1. Ouvrez la page Event Functions dans la console Lambda.
2. Choisissez une fonction Java pour laquelle vous souhaitez personnaliser la compilation par niveau.
3. Choisissez l'onglet Configuration, puis Variables d'environnement dans le menu de gauche.
4. Choisissez Modifier.
5. Choisissez Ajouter une variable d’environnement.
6. Pour Nom de la clé, saisissez `JAVA_TOOL_OPTIONS`. Pour Valeur, saisissez `-XX:+TieredCompilation -XX:TieredStopAtLevel=1`.



7. Cliquez sur Enregistrer.

> **Note**
>
> Vous pouvez également utiliser Lambda SnapStart pour atténuer les problèmes de démarrage à froid. SnapStartutilise des instantanés mis en cache de votre environnement d'exécution pour améliorer de manière significative les performances de démarrage. Pour plus d'informations sur les SnapStart fonctionnalités, les limitations et les régions prises en charge, consultezAméliorer les performances de démarrage avec Lambda SnapStart.

Exemple : personnalisation du comportement de GC à l'aide de JAVA_TOOL_OPTIONS

Les exécutions Java 11 utilisent le récupérateur de mémoire (GC) Serial pour la récupération de mémoire. Par défaut, les exécutions Java 17 utilisent également le GC Serial. Toutefois, avec Java 17, vous pouvez également utiliser la variable d'environnement `JAVA_TOOL_OPTIONS` pour modifier le GC par défaut. Vous pouvez choisir entre le GC Parallel et le GC Shenandoah.

Par exemple, si votre charge de travail utilise davantage de mémoire et plusieurs UC, envisagez d'utiliser le GC Parallel pour de obtenir de meilleures performances. Vous pouvez le faire en ajoutant ce qui suit à la valeur de votre variable d'environnement `JAVA_TOOL_OPTIONS` :

```
-XX:+UseParallelGC
```

Si votre charge de travail comporte de nombreux objets de courte durée, vous pouvez bénéficier d'une réduction de la consommation de mémoire en activant le mode générationnel du ramasse-miettes Shenandoah introduit dans Java 25. Pour ce faire, ajoutez ce qui suit à la valeur de votre variable d'`JAVA_TOOL_OPTIONS`environnement :

```
-XX:+UseShenandoahGC -XX:ShenandoahGCMode=generational
```

Patch Log4j pour Log4Shell

Les environnements d'exécution Lambda pour Java 8, 11, 17 et 21 incluent un correctif destiné à atténuer la vulnérabilité Log4Shell (CVE-2021-44228) dans Log4j, un framework de journalisation Java populaire. Ce correctif entraîne une surcharge des performances de démarrage à froid. Si vous utilisez une version corrigée de Log4j (version 2.17.0 ou ultérieure), vous pouvez désactiver ce correctif pour améliorer les performances de démarrage à froid. Pour désactiver le correctif, définissez la variable d'`AWS_LAMBDA_DISABLE_CVE_2021_44228_PROTECTION`environnement sur`true`.

À partir de Java 25, les environnements d'exécution Lambda n'incluent plus le correctif Log4Shell. Vous devez vérifier que vous utilisez Log4j version 2.17.0 ou ultérieure.

Ahead-of-Time (AOT) et caches CDS

À partir de Java 25, le moteur d'exécution Lambda inclut un cache Ahead-of-Time (AOT) pour le client d'interface d'exécution Java (RIC), un composant d'exécution qui interroge activement les événements provenant de l'API Lambda Runtime. Cela améliore les performances de démarrage à froid.

Les caches AOT sont spécifiques à une version de machine virtuelle Java. Lorsque Lambda met à jour le runtime géré, il met également à jour le cache AOT du RIC. Toutefois, si vous déployez vos propres caches AOT, ceux-ci peuvent être invalidés ou entraîner un comportement inattendu après une mise à jour d'exécution. Nous recommandons donc vivement de ne pas utiliser les caches AOT lorsque vous utilisez des environnements d'exécution gérés. Pour utiliser les caches AOT, vous devez déployer vos fonctions à l'aide d'images de conteneur.

Les caches AOT ne peuvent pas être utilisés avec les caches de partage de données de classe (CDS). Si vous déployez des caches CDS dans votre fonction Lambda, Lambda désactive le cache AOT.

Utilisation de l'objet de contexte Lambda pour récupérer les informations de la fonction d'événement Java

Lorsque Lambda exécute votre fonction, il transmet un objet contexte au gestionnaire. Cet objet fournit des méthodes et des propriétés fournissant des informations sur l'invocation, la fonction et l'environnement d'exécution.

Méthodes de contexte

- `getRemainingTimeInMillis()` – Renvoie le nombre de millisecondes restant avant l'expiration de l'exécution.
- `getFunctionName()` – Renvoie le nom de la fonction Lambda.
- `getFunctionVersion()` – Renvoie la version de la fonction.
- `getInvokedFunctionArn()` – Renvoie l'Amazon Resource Name (ARN) utilisé pour invoquer la fonction. Indique si l'appelant a spécifié un numéro de version ou un alias.
- `getMemoryLimitInMB()` – Renvoie la quantité de mémoire allouée à la fonction.
- `getAwsRequestId()` – Renvoie l'identifiant de la demande d'invocation.
- `getLogGroupName()` – Renvoie le groupe de journaux pour la fonction.
- `getLogStreamName()` – Renvoie le flux de journal de l'instance de fonction.
- `getIdentity()` – (applications mobiles) Renvoie des informations sur l'identité Amazon Cognito qui a autorisé la demande.
- `getClientContext()` – (applications mobiles) Renvoie le contexte client fourni à Lambda par l'application client.
- `getLogger()` – Renvoie l'objet enregistreur pour la fonction.

L'exemple suivant montre une fonction qui utilise l'objet contexte pour accéder à l'enregistreur Lambda.

Example Handler.java

```
package example;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.LambdaLogger;
import com.amazonaws.services.lambda.runtime.RequestHandler;

import java.util.Map;
```

```
// Handler value: example.Handler
public class Handler implements RequestHandler<Map<String,String>, Void>{

  @Override
  public Void handleRequest(Map<String,String> event, Context context)
  {
    LambdaLogger logger = context.getLogger();
    logger.log("EVENT TYPE: " + event.getClass());
    return null;
  }
}
```

La fonction enregistre le type de classe de l'événement entrant avant de le renvoyer `null`.

Example sortie de journal

```
EVENT TYPE: class java.util.LinkedHashMap
```

L'interface de l'objet contexte est disponible dans la bibliothèque aws-lambda-java-core. Vous pouvez implémenter cette interface pour créer une classe de contexte à des fins de test. L'exemple suivant montre une classe de contexte qui renvoie des valeurs factices pour la plupart des propriétés et un enregistreur de test opérationnel.

Example src/test/java/example/TestContext.java

```
package example;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.CognitoIdentity;
import com.amazonaws.services.lambda.runtime.ClientContext;
import com.amazonaws.services.lambda.runtime.LambdaLogger;

public class TestContext implements Context{

  public TestContext() {}
  public String getAwsRequestId(){
    return new String("495b12a8-xmpl-4eca-8168-160484189f99");
  }
  public String getLogGroupName(){
    return new String("/aws/lambda/my-function");
  }
  public String getLogStreamName(){
```

```
    return new String("2020/02/26/[$LATEST]704f8dxmpla04097b9134246b8438f1a");
  }
  public String getFunctionName(){
    return new String("my-function");
  }
  public String getFunctionVersion(){
    return new String("$LATEST");
  }
  public String getInvokedFunctionArn(){
    return new String("arn:aws:lambda:us-east-2:123456789012:function:my-function");
  }
  public CognitoIdentity getIdentity(){
    return null;
  }
  public ClientContext getClientContext(){
    return null;
  }
  public int getRemainingTimeInMillis(){
    return 300000;
  }
  public int getMemoryLimitInMB(){
    return 512;
  }
  public LambdaLogger getLogger(){
    return new TestLogger();
  }

}
```

Pour de plus amples informations sur la journalisation, veuillez consulter Enregistrez et surveillez les fonctions d'événements Java Lambda.

Contexte dans des exemples d'applications

Le GitHub référentiel de ce guide inclut des exemples d'applications illustrant l'utilisation de l'objet de contexte. Chaque exemple d'application inclut des scripts pour faciliter le déploiement et le nettoyage, un modèle AWS Serverless Application Model (AWS SAM) et des ressources de support.

Exemples d’applications Lambda en Java

- example-java — Une fonction d'événement Java qui montre comment utiliser Lambda pour traiter les commandes. Cette fonction montre comment définir et désérialiser un objet d'événement d'entrée personnalisé, utiliser le AWS SDK et enregistrer les sorties.

- java-basic – Ensemble de fonctions Java minimales avec des tests unitaires et une configuration de journalisation variable.
- java events – Ensemble de fonctions Java contenant du code squelette permettant de gérer les événements de divers services tels qu'Amazon API Gateway, Amazon SQS et Amazon Kinesis. Ces fonctions utilisent la dernière version (3.0.0 et ultérieure) de la bibliothèque aws-lambda-java-events. Ces exemples ne nécessitent pas le AWS SDK comme dépendance.
- s3-java – Fonction Java qui traite les événements de notification d'Amazon S3 et utilise la bibliothèque de classes Java (JCL) pour créer des miniatures à partir de fichiers d'image chargés.
- layer-java : fonction Java qui illustre comment utiliser une couche Lambda pour empaqueter les dépendances séparément du code de votre fonction principale.

Enregistrez et surveillez les fonctions d'événements Java Lambda

AWS Lambda surveille automatiquement les fonctions Lambda et envoie des entrées de journal à Amazon. CloudWatch Votre fonction Lambda est fournie avec un groupe de CloudWatch journaux Logs et un flux de journaux pour chaque instance de votre fonction. L'environnement d'exécution Lambda envoie des détails sur chaque invocation et d'autres sorties provenant du code de votre fonction au flux de journaux. Pour plus d'informations sur CloudWatch les journaux, consultezEnvoi des journaux des fonctions d'événements Lambda aux journaux CloudWatch.

Pour produire des journaux à partir de votre code de fonction, vous pouvez utiliser des méthodes sur java.lang.System, ou tout module de journalisation qui écrit sur stdout ou stderr.

Sections

- Création d'une fonction qui renvoie des journaux
- Utilisation des contrôles de journalisation avancés de Lambda avec Java
- Implémentation de la journalisation avancée avec Log4j2 et SLF4J
- Utilisation d'autres outils et bibliothèques de journalisation
- Utilisation de Powertools pour AWS Lambda (Java) et AWS SAM pour une journalisation structurée
- Affichage des journaux dans la console Lambda
- Afficher les journaux dans la CloudWatch console
- Afficher les journaux à l'aide du AWS Command Line Interface (AWS CLI)
- Suppression de journaux
- Exemple de code de journalisation

Création d'une fonction qui renvoie des journaux

Pour générer les journaux à partir de votre code de fonction, vous pouvez utiliser des méthodes sur java.lang.System ou n'importe quelle bibliothèque de journalisation qui écrit dans `stdout` ou `stderr`. La bibliothèque aws-lambda-java-core fournit une classe d'enregistreur nommée `LambdaLogger` à laquelle vous pouvez accéder à partir de l'objet de contexte. La classe d'enregistreur prend en charge les journaux multilignes.

L'exemple suivant utilise l'enregistreur `LambdaLogger` fourni par l'objet de contexte.

Example Handler.java

```
// Handler value: example.Handler
```

```
public class Handler implements RequestHandler<Object, String>{
  Gson gson = new GsonBuilder().setPrettyPrinting().create();
  @Override
  public String handleRequest(Object event, Context context)
  {
    LambdaLogger logger = context.getLogger();
    String response = new String("SUCCESS");
    // log execution details
    logger.log("ENVIRONMENT VARIABLES: " + gson.toJson(System.getenv()));
    logger.log("CONTEXT: " + gson.toJson(context));
    // process event
    logger.log("EVENT: " + gson.toJson(event));
    return response;
  }
}
```

Example format des journaux

```
START RequestId: 6bc28136-xmpl-4365-b021-0ce6b2e64ab0 Version: $LATEST
ENVIRONMENT VARIABLES:
{
    "_HANDLER": "example.Handler",
    "AWS_EXECUTION_ENV": "AWS_Lambda_java8",
    "AWS_LAMBDA_FUNCTION_MEMORY_SIZE": "512",
    ...
}
CONTEXT:
{
    "memoryLimit": 512,
    "awsRequestId": "6bc28136-xmpl-4365-b021-0ce6b2e64ab0",
    "functionName": "java-console",
    ...
}
EVENT:
{
  "records": [
    {
      "messageId": "19dd0b57-xmpl-4ac1-bd88-01bbb068cb78",
      "receiptHandle": "MessageReceiptHandle",
      "body": "Hello from SQS!",
       ...
    }
  ]
```

```
}
END RequestId: 6bc28136-xmpl-4365-b021-0ce6b2e64ab0
REPORT RequestId: 6bc28136-xmpl-4365-b021-0ce6b2e64ab0 Duration: 198.50 ms Billed
 Duration: 724 ms Memory Size: 512 MB Max Memory Used: 90 MB Init Duration: 524.75 ms
```

L'environnement d'exécution Java enregistre les lignes `START`, `END` et `REPORT` pour chaque invocation. La ligne de rapport fournit les détails suivants.

Champs de données de la ligne REPORT

- RequestId— L'identifiant de demande unique pour l'invocation.
- Duration – Temps que la méthode de gestion du gestionnaire de votre fonction a consacré au traitement de l'événement.
- Billed Duration : temps facturé pour l'invocation.
- Memory Size – Quantité de mémoire allouée à la fonction.
- Max Memory Used – Quantité de mémoire utilisée par la fonction. Lorsque les appels partagent un environnement d'exécution, Lambda indique la mémoire maximale utilisée pour toutes les invocations. Ce comportement peut entraîner une valeur signalée plus élevée que prévu.
- Init Duration : pour la première requête servie, temps qu'il a pris à l'exécution charger la fonction et exécuter le code en dehors de la méthode du gestionnaire.
- XRAY TraceId — Pour les demandes suivies, l'ID de AWS X-Ray trace.
- SegmentId— Pour les demandes suivies, l'ID X-Ray du segment.
- Sampled : pour les demandes suivies, résultat de l'échantillonnage.

Utilisation des contrôles de journalisation avancés de Lambda avec Java

Pour mieux contrôler la manière dont les journaux de vos fonctions sont capturés, traités et consommés, vous pouvez configurer les options de journalisation suivantes pour les environnements d'exécution Java pris en charge :

- Format de journal : choisissez entre le format texte brut et le format JSON structuré pour les journaux de votre fonction
- Niveau du journal : pour les journaux au format JSON, choisissez le niveau de détail des journaux auxquels Lambda envoie CloudWatch, par exemple ERROR, DEBUG ou INFO
- Groupe de journaux : choisissez le groupe de CloudWatch journaux auquel votre fonction envoie les journaux

Pour plus d'informations sur ces options de journalisation et pour savoir comment configurer votre fonction pour les utiliser, consultez the section called "Configuration de contrôles de journalisation avancés pour les fonctions d'événement Lambda".

Pour utiliser le format de journal et les options de niveau de journal avec vos fonctions Java Lambda, consultez les instructions des sections suivantes.

Utilisation du format de journal JSON structuré avec Java

Si vous sélectionnez JSON pour le format de journal de votre fonction, Lambda envoie la sortie des journaux en utilisant la `LambdaLogger` classe sous forme de JSON structuré. Chaque objet de journal JSON contient au moins quatre paires clé-valeur avec les clés suivantes :

- `"timestamp"` - heure à laquelle le message de journal a été généré
- `"level"` - niveau de journalisation attribué au message
- `"message"` - contenu du message de journal
- `"AWSrequestId"` - identifiant unique de la demande pour l'invocation de la fonction

Selon la méthode de journalisation que vous utilisez, les sorties de journal de votre fonction capturées au format JSON peuvent également contenir des paires clé-valeur supplémentaires.

Pour attribuer un niveau aux journaux que vous créez à l'aide de l'enregistreur `LambdaLogger`, vous devez fournir un argument `LogLevel` dans votre commande de journalisation, comme illustré dans l'exemple suivant.

Example Code de journalisation Java

```
LambdaLogger logger = context.getLogger();
logger.log("This is a debug log", LogLevel.DEBUG);
```

Cette sortie de journal produite par cet exemple de code serait capturée dans CloudWatch Logs comme suit :

Example Enregistrement de journaux JSON

```
{
    "timestamp":"2023-11-01T00:21:51.358Z",
    "level":"DEBUG",
```

```
    "message":"This is a debug log",
    "AWSrequestId":"93f25699-2cbf-4976-8f94-336a0aa98c6f"
}
```

Si vous n'attribuez aucun niveau à la sortie de votre journal, Lambda lui attribue automatiquement le niveau INFO.

Si votre code utilise déjà une autre bibliothèque de journalisation pour produire des journaux structurés en JSON, vous n'avez pas besoin d'apporter de modifications. Lambda ne double code aucun journal déjà codé au format JSON. Même si vous configurez votre fonction pour utiliser le format de journal JSON, vos sorties de journalisation apparaissent CloudWatch dans la structure JSON que vous définissez.

Utilisation du filtrage au niveau du journal avec Java

AWS Lambda Pour filtrer les journaux de votre application en fonction de leur niveau de journalisation, votre fonction doit utiliser des journaux au format JSON. Vous pouvez effectuer cette opération de deux façons :

- Créez des sorties de journal à l'aide de la norme `LambdaLogger` et configurez votre fonction pour utiliser le format de journal JSON. Lambda filtre ensuite les sorties de votre journal à l'aide de la paire clé-valeur « niveau » de l'objet JSON décrit dans. the section called “Utilisation du format de journal JSON structuré avec Java” Pour savoir comment configurer le format de journal de votre fonction, consultezthe section called “Configuration de contrôles de journalisation avancés pour les fonctions d'événement Lambda”.
- Utilisez une autre bibliothèque ou méthode de journalisation pour créer des journaux structurés JSON dans votre code qui incluent une paire clé-valeur « niveau » définissant le niveau de sortie du journal. Vous pouvez utiliser n'importe quelle bibliothèque de journalisation qui écrit des journaux JSON dans `stdout` ou `stderr`. Par exemple, vous pouvez utiliser Powertools for AWS Lambda ou le package Log4j2 pour générer des sorties de journal structurées JSON à partir de votre code. Pour en savoir plus, consultez the section called “Utilisation de Powertools pour AWS Lambda (Java) et AWS SAM pour une journalisation structurée” et the section called “Implémentation de la journalisation avancée avec Log4j2 et SLF4J”.

Lorsque vous configurez votre fonction pour utiliser le filtrage au niveau des journaux, vous devez sélectionner l'une des options suivantes pour le niveau de journaux que Lambda doit envoyer à Logs : CloudWatch

Niveau de journalisation	Utilisation standard
TRACE (le plus détaillé)	Les informations les plus précises utilisées pour tracer le chemin d'exécution de votre code
DEBUG	Informations détaillées pour le débogage du système
INFO	Messages qui enregistrent le fonctionnement normal de votre fonction
WARN	Messages relatifs à des erreurs potentielles susceptibles d'entraîner un comportement inattendu si elles ne sont pas traitées
ERROR	Messages concernant les problèmes qui empêchent le code de fonctionner comme prévu
FATAL (moindre détail)	Messages relatifs à des erreurs graves entraînant l'arrêt du fonctionnement de l'applica tion

Pour que Lambda puisse filtrer les journaux de votre fonction, vous devez également inclure une paire `"timestamp"` clé-valeur dans la sortie de votre journal JSON. L'heure doit être spécifiée dans un format d'horodatage RFC 3339 valide. Si vous ne fournissez pas d'horodatage valide, Lambda attribue au journal le niveau INFO et ajoute un horodatage pour vous.

Lambda envoie les journaux du niveau sélectionné et d'un niveau inférieur à. CloudWatch Par exemple, si vous configurez un niveau de journalisation WARN, Lambda envoie des journaux correspondant aux niveaux WARN, ERROR et FATAL.

Implémentation de la journalisation avancée avec Log4j2 et SLF4J

> **Note**
>
> AWS Lambda n'inclut pas Log4j2 dans ses environnements d'exécution gérés ni dans ses images de conteneur de base. Ils ne sont donc pas concernés par les problèmes décrits dans CVE-2021-44228 CVE-2021-45046, et CVE-2021-45105.
> Dans les cas où une fonction client inclut une version de Log4j2 affectée, nous avons apporté une modification aux environnements d'exécution gérés par Lambda Java et aux images de conteneur de base afin d'atténuer les problèmes liés à, et. CVE-2021-44228 CVE-2021-45046 CVE-2021-45105 À la suite de cette modification, les clients utilisant Log4J2 peuvent voir une entrée de journal supplémentaire, similaire à « `Transforming org/apache/logging/log4j/core/lookup/JndiLookup (java.net.URLClassLoader@...)` ». Toutes les chaînes de log faisant référence au mappeur jndi dans la sortie Log4J2 sont remplacées par « ». `Patched JndiLookup::lookup()`
> Indépendamment de ce changement, nous encourageons vivement tous les clients dont les fonctions incluent Log4j2 à mettre à jour vers la dernière version. Plus précisément, les clients utilisant la bibliothèque aws-lambda-java-log4j2 dans leurs fonctions doivent effectuer une mise à jour vers la version 1.5.0 (ou ultérieure) et redéployer leurs fonctions. Cette version met à jour les dépendances sous-jacentes de l'utilitaire Log4j2 vers la version 2.17.0 (ou ultérieure). Le binaire aws-lambda-java-log4j2 mis à jour est disponible dans le dépôt Maven tandis que son code source est disponible dans Github.
> Enfin, notez que les bibliothèques associées à aws-lambda-java-log4j (v1.0.0 ou 1.0.1) ne doivent en aucun cas être utilisées. Ces bibliothèques sont liées à la version 1.x de log4j qui a pris fin en 2015. Les bibliothèques ne sont pas prises en charge, ne sont pas maintenues, ne sont pas corrigées et présentent des failles de sécurité connues.

Pour personnaliser la sortie du journal, prendre en charge la journalisation pendant les tests unitaires et enregistrer les appels du AWS SDK, utilisez Apache Log4j2 avec SLF4J. Log4j est une bibliothèque de journalisation pour les programmes Java que vous pouvez utiliser pour configurer les niveaux de journalisation et utiliser des bibliothèques d'annexes. SLF4J est une bibliothèque de façade que vous pouvez utiliser pour changer la bibliothèque que vous utilisez sans changer le code de votre fonction.

Pour ajouter l'ID de requête aux journaux de votre fonction, utilisez l'appender dans la bibliothèque aws-lambda-java-log4j2.

Example src/main/resources/log4j2.xml — Configuration de l'annexe

```
<Configuration>
  <Appenders>
    <Lambda name="Lambda" format="${env:AWS_LAMBDA_LOG_FORMAT:-TEXT}">
       <LambdaTextFormat>
         <PatternLayout>
             <pattern>%d{yyyy-MM-dd HH:mm:ss} %X{AWSRequestId} %-5p %c{1} - %m%n </
pattern>
         </PatternLayout>
       </LambdaTextFormat>
       <LambdaJSONFormat>
         <JsonTemplateLayout eventTemplateUri="classpath:LambdaLayout.json" />
       </LambdaJSONFormat>
     </Lambda>
   </Appenders>
   <Loggers>
     <Root level="${env:AWS_LAMBDA_LOG_LEVEL:-INFO}">
       <AppenderRef ref="Lambda"/>
     </Root>
     <Logger name="software.amazon.awssdk" level="WARN" />
     <Logger name="software.amazon.awssdk.request" level="DEBUG" />
   </Loggers>
 </Configuration>
```

Vous pouvez décider comment vos journaux Log4j2 sont configurés pour les sorties en texte brut ou JSON en spécifiant une mise en page sous les balises `<LambdaTextFormat>` et `<LambdaJSONFormat>`.

Dans cet exemple, en mode texte, chaque ligne est précédée de la date, de l'heure, de l'ID de demande, du niveau de journal et du nom de classe. En mode JSON, `<JsonTemplateLayout>` est utilisé avec une configuration fournie avec la bibliothèque `aws-lambda-java-log4j2`.

SLF4J est une bibliothèque de façade pour la journalisation en code Java. Dans votre code de fonction, vous utilisez la fabrique d'enregistreurs SLF4J pour récupérer un enregistreur avec des méthodes pour les niveaux de journalisation comme `info()` et `warn()`. Dans votre configuration de build, vous incluez la bibliothèque de journalisation et l'adaptateur SLF4J dans le chemin de classe. En changeant les bibliothèques dans la configuration de build, vous pouvez changer le type d'enregistreur sans changer votre code de fonction. SLF4J est nécessaire pour capturer les journaux du kit SDK pour Java.

Dans l'exemple de code suivant, la classe de gestionnaire utilise SLF4J pour récupérer un enregistreur.

Example src/main/java/example/HandlerS3.java — Journalisation avec SLF4J

```
package example;

import org.slf4j.Logger;
import org.slf4j.LoggerFactory;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.S3Event;

import static org.apache.logging.log4j.CloseableThreadContext.put;


public class HandlerS3 implements RequestHandler<S3Event, String>{
    private static final Logger logger = LoggerFactory.getLogger(HandlerS3.class);

    @Override
    public String handleRequest(S3Event event, Context context) {
        for(var record : event.getRecords()) {
            try (var loggingCtx = put("awsRegion", record.getAwsRegion())) {
                loggingCtx.put("eventName", record.getEventName());
                loggingCtx.put("bucket", record.getS3().getBucket().getName());
                loggingCtx.put("key", record.getS3().getObject().getKey());

                logger.info("Handling s3 event");
            }
        }

        return "Ok";
    }
}
```

Ce code produit des sorties de journal similaires à ce qui suit :

Example format des journaux

```
{
    "timestamp": "2023-11-15T16:56:00.815Z",
    "level": "INFO",
```

```
    "message": "Handling s3 event",
    "logger": "example.HandlerS3",
    "AWSRequestId": "0bced576-3936-4e5a-9dcd-db9477b77f97",
    "awsRegion": "eu-south-1",
    "bucket": "java-logging-test-input-bucket",
    "eventName": "ObjectCreated:Put",
    "key": "test-folder/"
}
```

La configuration de build prend des dépendances d'exécution sur l'appender Lambda et l'adaptateur SLF4J, et des dépendances d'implémentation sur Log4j2.

Example build.gradle – Dépendances de journalisation

```
dependencies {
    ...
    'com.amazonaws:aws-lambda-java-log4j2:[1.6.0,)',
    'com.amazonaws:aws-lambda-java-events:[3.11.3,)',
    'org.apache.logging.log4j:log4j-layout-template-json:[2.17.1,)',
    'org.apache.logging.log4j:log4j-slf4j2-impl:[2.19.0,)',
    ...
}
```

Lorsque vous exécutez votre code localement pour des tests, l'objet contecte avec l'enregistreur Lambda n'est pas disponible, et il n'y a pas d'ID de requête que l'appender Lambda puisse utiliser. Pour des exemples de configurations de test, consultez les exemples d'applications dans la section suivante.

Utilisation d'autres outils et bibliothèques de journalisation

Powertools for AWS Lambda (Java) est une boîte à outils destinée aux développeurs qui permet de mettre en œuvre les meilleures pratiques sans serveur et d'accroître la rapidité des développeurs. L'utilitaire Logging (français non garanti) fournit un enregistreur optimisé pour Lambda qui inclut des informations supplémentaires sur le contexte de fonction pour toutes vos fonctions avec une sortie structurée en JSON. Utilisez cet utilitaire pour effectuer les opérations suivantes :

- Capturer les champs clés du contexte Lambda, démarrer à froid et structurer la sortie de la journalisation sous forme de JSON
- Journaliser les événements d'invocation Lambda lorsque cela est demandé (désactivé par défaut)
- Imprimer tous les journaux uniquement pour un pourcentage d'invocations via l'échantillonnage des journaux (désactivé par défaut)

- Ajouter des clés supplémentaires au journal structuré à tout moment
- Utiliser un formateur de journaux personnalisé (Apportez votre propre formateur) pour produire des journaux dans une structure compatible avec le RFC de journalisation de votre organisation

Utilisation de Powertools pour AWS Lambda (Java) et AWS SAM pour une journalisation structurée

Suivez les étapes ci-dessous pour télécharger, créer et déployer un exemple d'application Java Hello World avec des modules Powertools for AWS Lambda (Java) intégrés à l'aide du AWS SAM. Cette application met en œuvre un backend API de base et utilise Powertools pour émettre des journaux, des métriques et des traces. Il se compose d'un point de terminaison Amazon API Gateway et d'une fonction d'événement Lambda. Lorsque vous envoyez une requête GET au point de terminaison API Gateway, la fonction Lambda appelle, envoie des journaux et des métriques au format métrique intégré à CloudWatch, et envoie des traces à. AWS X-Ray La fonction renvoie un message `hello world`.

Conditions préalables

Pour exécuter la procédure indiquée dans cette section, vous devez satisfaire aux exigences suivantes :

- Java 11
- AWS CLI version 2
- AWS SAM CLI version 1.75 ou ultérieure. Si vous disposez d'une ancienne version de la AWS SAM CLI, reportez-vous à la section Mise à niveau de la AWS SAM CLI.

Déployer un échantillon AWS SAM vigie

1. Initialisez l'application à l'aide du modèle Hello World Java.

```
sam init --app-template hello-world-powertools-java --name sam-app --package-type
 Zip --runtime java11 --no-tracing
```

2. Créez l'application.

```
cd sam-app && sam build
```

3. Déployez l'application.

```
sam deploy --guided
```

4. Suivez les invites à l'écran. Appuyez sur `Enter` pour accepter les options par défaut fournies dans l'expérience interactive.

> **Note**
>
> Car l'autorisation n'a HelloWorldFunction peut-être pas été définie, est-ce que ça va ? , assurez-vous de participery.

5. Obtenez l'URL de l'application déployée :

```
aws cloudformation describe-stacks --stack-name sam-app --query
 'Stacks[0].Outputs[?OutputKey==`HelloWorldApi`].OutputValue' --output text
```

6. Invoquez le point de terminaison de l'API :

```
curl -X GET <URL_FROM_PREVIOUS_STEP>
```

En cas de succès, vous obtiendrez cette réponse :

```
{"message":"hello world"}
```

7. Pour obtenir les journaux de la fonction, exécutez sam logs. Pour en savoir plus, consultez Utilisation des journaux dans le Guide du développeur AWS Serverless Application Model .

```
sam logs --stack-name sam-app
```

La sortie du journal se présente comme suit :

```
2025/09/03/[$LATEST]851411a899b545eea2cffeba4cfbec81 2023-02-03T09:24:34.095000
 INIT_START Runtime Version: java:11.v15    Runtime Version ARN: arn:aws:lambda:eu-
central-1::runtime:0a25e3e7a1cc9ce404bc435eeb2ad358d8fa64338e618d0c224fe509403583ca
2025/09/03/[$LATEST]851411a899b545eea2cffeba4cfbec81 2023-02-03T09:24:34.114000
 Picked up JAVA_TOOL_OPTIONS: -XX:+TieredCompilation -XX:TieredStopAtLevel=1
2025/09/03/[$LATEST]851411a899b545eea2cffeba4cfbec81 2023-02-03T09:24:34.793000
 Transforming org/apache/logging/log4j/core/lookup/JndiLookup
 (lambdainternal.CustomerClassLoader@1a6c5a9e)
```

```
2025/09/03/[$LATEST]851411a899b545eea2cffeba4cfbec81 2023-02-03T09:24:35.252000
 START RequestId: 7fcf1548-d2d4-41cd-a9a8-6ae47c51f765 Version: $LATEST
2025/09/03/[$LATEST]851411a899b545eea2cffeba4cfbec81 2023-02-03T09:24:36.531000 {
  "_aws": {
    "Timestamp": 1675416276051,
    "CloudWatchMetrics": [
      {
        "Namespace": "sam-app-powerools-java",
        "Metrics": [
          {
            "Name": "ColdStart",
            "Unit": "Count"
          }
        ],
        "Dimensions": [
          [
            "Service",
            "FunctionName"
          ]
        ]
      }
    ]
  },
  "function_request_id": "7fcf1548-d2d4-41cd-a9a8-6ae47c51f765",
  "traceId":
 "Root=1-63dcd2d1-25f90b9d1c753a783547f4dd;Parent=e29684c1be352ce4;Sampled=1",
  "FunctionName": "sam-app-HelloWorldFunction-y9Iu1FLJJBGD",
  "functionVersion": "$LATEST",
  "ColdStart": 1.0,
  "Service": "service_undefined",
  "logStreamId": "2025/09/03/[$LATEST]851411a899b545eea2cffeba4cfbec81",
  "executionEnvironment": "AWS_Lambda_java11"
}
2025/09/03/[$LATEST]851411a899b545eea2cffeba4cfbec81 2023-02-03T09:24:36.974000 Feb
 03, 2023 9:24:36 AM com.amazonaws.xray.AWSXRayRecorder <init>
2025/09/03/[$LATEST]851411a899b545eea2cffeba4cfbec81 2023-02-03T09:24:36.993000 Feb
 03, 2023 9:24:36 AM com.amazonaws.xray.config.DaemonConfiguration <init>
2025/09/03/[$LATEST]851411a899b545eea2cffeba4cfbec81 2023-02-03T09:24:36.993000
 INFO: Environment variable AWS_XRAY_DAEMON_ADDRESS is set. Emitting to daemon on
 address XXXX.XXXX.XXXX.XXXX:2000.
2025/09/03/[$LATEST]851411a899b545eea2cffeba4cfbec81 2023-02-03T09:24:37.331000
 09:24:37.294 [main] INFO  helloworld.App - {"version":null,"resource":"/
hello","path":"/hello/","httpMethod":"GET","headers":{"Accept":"*/
*","CloudFront-Forwarded-Proto":"https","CloudFront-Is-Desktop-
```

```
Viewer":"true","CloudFront-Is-Mobile-Viewer":"false","CloudFront-Is-
SmartTV-Viewer":"false","CloudFront-Is-Tablet-Viewer":"false","CloudFront-
Viewer-ASN":"16509","CloudFront-Viewer-Country":"IE","Host":"XXXX.execute-
api.eu-central-1.amazonaws.com","User-Agent":"curl/7.86.0","Via":"2.0
 f0300a9921a99446a44423d996042050.cloudfront.net (CloudFront)","X-Amz-
Cf-Id":"t9W5ByT11HaY33NM8YioKECn_4eMpNsOMPfEVRczD7T1RdhbtiwV1Q==","X-
Amzn-Trace-Id":"Root=1-63dcd2d1-25f90b9d1c753a783547f4dd","X-Forwarded-
For":"XX.XXX.XXX.XX, XX.XXX.XXX.XX","X-Forwarded-Port":"443","X-
Forwarded-Proto":"https"},"multiValueHeaders":{"Accept":["*/
*"],"CloudFront-Forwarded-Proto":["https"],"CloudFront-Is-Desktop-Viewer":
["true"],"CloudFront-Is-Mobile-Viewer":["false"],"CloudFront-Is-SmartTV-
Viewer":["false"],"CloudFront-Is-Tablet-Viewer":["false"],"CloudFront-Viewer-
ASN":["16509"],"CloudFront-Viewer-Country":["IE"],"Host":["XXXX.execute-
api.eu-central-1.amazonaws.com"],"User-Agent":["curl/7.86.0"],"Via":["2.0
 f0300a9921a99446a44423d996042050.cloudfront.net (CloudFront)"],"X-Amz-
Cf-Id":["t9W5ByT11HaY33NM8YioKECn_4eMpNsOMPfEVRczD7T1RdhbtiwV1Q=="],"X-
Amzn-Trace-Id":["Root=1-63dcd2d1-25f90b9d1c753a783547f4dd"],"X-Forwarded-
For":["XXX, XXX"],"X-Forwarded-Port":["443"],"X-Forwarded-Proto":
["https"]},"queryStringParameters":null,"multiValueQueryStringParameters":null,"pathParamet
{"accountId":"XXX","stage":"Prod","resourceId":"at73a1","requestId":"ba09ecd2-
acf3-40f6-89af-fad32df67597","operationName":null,"identity":
{"cognitoIdentityPoolId":null,"accountId":null,"cognitoIdentityId":null,"caller":null,"apiK
hello","httpMethod":"GET","apiId":"XXX","path":"/Prod/
hello/","authorizer":null},"body":null,"isBase64Encoded":false}
2025/09/03/[$LATEST]851411a899b545eea2cffeba4cfbec81 2023-02-03T09:24:37.351000
 09:24:37.351 [main] INFO  helloworld.App - Retrieving https://
checkip.amazonaws.com
2025/09/03/[$LATEST]851411a899b545eea2cffeba4cfbec81 2023-02-03T09:24:39.313000 {
  "function_request_id": "7fcf1548-d2d4-41cd-a9a8-6ae47c51f765",
  "traceId":
 "Root=1-63dcd2d1-25f90b9d1c753a783547f4dd;Parent=e29684c1be352ce4;Sampled=1",
  "xray_trace_id": "1-63dcd2d1-25f90b9d1c753a783547f4dd",
  "functionVersion": "$LATEST",
  "Service": "service_undefined",
  "logStreamId": "2025/09/03/[$LATEST]851411a899b545eea2cffeba4cfbec81",
  "executionEnvironment": "AWS_Lambda_java11"
}
2025/09/03/[$LATEST]851411a899b545eea2cffeba4cfbec81 2023-02-03T09:24:39.371000 END
 RequestId: 7fcf1548-d2d4-41cd-a9a8-6ae47c51f765
2025/09/03/[$LATEST]851411a899b545eea2cffeba4cfbec81 2023-02-03T09:24:39.371000
 REPORT RequestId: 7fcf1548-d2d4-41cd-a9a8-6ae47c51f765    Duration: 4118.98 ms
 Billed Duration: 5275 ms    Memory Size: 512 MB    Max Memory Used: 152 MB    Init
 Duration: 1155.47 ms
```

```
XRAY TraceId: 1-63dcd2d1-25f90b9d1c753a783547f4dd    SegmentId: 3a028fee19b895cb
 Sampled: true
```

8. Il s'agit d'un point de terminaison d'API public accessible par Internet. Nous vous recommandons de supprimer le point de terminaison après un test.

```
sam delete
```

Gestion de la conservation des journaux

Les groupes de journaux ne sont pas supprimés automatiquement quand vous supprimez une fonction. Pour éviter de stocker les journaux indéfiniment, supprimez le groupe de journaux ou configurez une période de conservation après laquelle les journaux CloudWatch sont automatiquement supprimés. Pour configurer la conservation des journaux, ajoutez ce qui suit à votre AWS SAM modèle :

```
Resources:
  HelloWorldFunction:
    Type: AWS::Serverless::Function
    Properties:
      # Omitting other properties

  LogGroup:
    Type: AWS::Logs::LogGroup
    Properties:
      LogGroupName: !Sub "/aws/lambda/${HelloWorldFunction}"
      RetentionInDays: 7
```

Affichage des journaux dans la console Lambda

Vous pouvez utiliser la console Lambda pour consulter les résultats du journal après avoir invoqué une fonction d'événement Lambda.

Si votre code peut être testé à partir de l'éditeur de code intégré, vous trouverez des journaux dans les résultats d'exécution. Lorsque vous utilisez la fonctionnalité de test de la console pour appeler une fonction, vous trouverez la sortie du journal dans la section Détails.

Afficher les journaux dans la CloudWatch console

Vous pouvez utiliser la CloudWatch console Amazon pour consulter les journaux de toutes les invocations de la fonction d'événement Lambda.

Pour afficher les journaux sur la CloudWatch console

1. Ouvrez la page Groupes de journaux sur la CloudWatch console.
2. Choisissez le groupe de journaux pour votre fonction (/aws/lambda/***your-function-name***).
3. Choisissez un flux de journaux.

Chaque flux de journal correspond à une instance de votre fonction. Un flux de journal apparaît lorsque vous mettez à jour votre fonction Lambda et lorsque des instances supplémentaires sont créées pour gérer les appels simultanés. Pour trouver les journaux d'un appel spécifique, nous vous recommandons d'instrumenter votre fonction avec. AWS X-Ray X-Ray enregistre les détails de la demande et du flux de log dans le traçage.

Afficher les journaux à l'aide du AWS Command Line Interface (AWS CLI)

AWS CLI Il s'agit d'un outil open source que vous pouvez utiliser pour interagir avec les AWS services à l'aide de commandes dans votre interface de ligne de commande. Pour effectuer les étapes de cette section, vous devez disposer de la version 2 de l'AWS CLI.

Vous pouvez utiliser AWS CLI pour récupérer les journaux d'une invocation à l'aide de l'option de commande `--log-type`. La réponse inclut un champ `LogResult` qui contient jusqu'à 4 Ko de journaux codés en base64 provenant de l'invocation.

Example récupérer un ID de journal

L'exemple suivant montre comment récupérer un ID de journal à partir du champ `LogResult` d'une fonction nommée `my-function`.

```
aws lambda invoke --function-name my-function out --log-type Tail
```

Vous devriez voir la sortie suivante:

```
{
    "StatusCode": 200,
    "LogResult":
 "U1RBUlQgUmVxdWVzdElkOiA4N2QwNDRiOC1mMTU0LTExZTgtOGNkYS0yOTc0YzVlNGZiMjEgVmVyc2lvb...",
    "ExecutedVersion": "$LATEST"
}
```

Example décoder les journaux

Dans la même invite de commandes, utilisez l'utilitaire `base64` pour décoder les journaux. L'exemple suivant montre comment récupérer les journaux encodés en base64 pour `my-function`.

```
aws lambda invoke --function-name my-function out --log-type Tail \
--query 'LogResult' --output text --cli-binary-format raw-in-base64-out | base64 --
decode
```

L'cli-binary-formatoption est obligatoire si vous utilisez AWS CLI la version 2. Pour faire de ce paramètre le paramètre par défaut, exécutez `aws configure set cli-binary-format raw-in-base64-out`. Pour plus d'informations, consultez les options de ligne de commande globales AWS CLI prises en charge dans le Guide de l'utilisateur AWS Command Line Interface version 2.

Vous devriez voir la sortie suivante :

```
START RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8 Version: $LATEST
"AWS_SESSION_TOKEN": "AgoJb3JpZ2luX2VjELj...", "_X_AMZN_TRACE_ID": "Root=1-5d02e5ca-
f5792818b6fe8368e5b51d50;Parent=191db58857df8395;Sampled=0"",ask/lib:/opt/lib",
END RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8
REPORT RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8  Duration: 79.67 ms      Billed
 Duration: 80 ms         Memory Size: 128 MB     Max Memory Used: 73 MB
```

L'utilitaire `base64` est disponible sous Linux, macOS et Ubuntu sous Windows. Les utilisateurs de macOS auront peut-être besoin d'utiliser `base64 -D`.

Example Script get-logs.sh

Dans la même invite de commandes, utilisez le script suivant pour télécharger les cinq derniers événements de journalisation. Le script utilise `sed` pour supprimer les guillemets du fichier de sortie et attend 15 secondes pour permettre la mise à disposition des journaux. La sortie comprend la réponse de Lambda, ainsi que la sortie de la commande `get-log-events`.

Copiez le contenu de l'exemple de code suivant et enregistrez-le dans votre répertoire de projet Lambda sous `get-logs.sh`.

L'cli-binary-formatoption est obligatoire si vous utilisez AWS CLI la version 2. Pour faire de ce paramètre le paramètre par défaut, exécutez `aws configure set cli-binary-format raw-in-base64-out`. Pour plus d'informations, consultez les options de ligne de commande globales AWS CLI prises en charge dans le Guide de l'utilisateur AWS Command Line Interface version 2.

```
#!/bin/bash
aws lambda invoke --function-name my-function --cli-binary-format raw-in-base64-out --
payload '{"key": "value"}' out
sed -i'' -e 's/"//g' out
sleep 15
aws logs get-log-events --log-group-name /aws/lambda/my-function --log-stream-
name stream1 --limit 5
```

Example macOS et Linux (uniquement)

Dans la même invite de commande, les utilisateurs de macOS et de Linux devront peut-être exécuter la commande suivante pour s'assurer que le script est exécutable.

```
chmod -R 755 get-logs.sh
```

Example récupérer les cinq derniers événements de journal

Dans la même invite de commande, exécutez le script suivant pour obtenir les cinq derniers événements de journalisation.

```
./get-logs.sh
```

Vous devriez voir la sortie suivante:

```
{
    "StatusCode": 200,
    "ExecutedVersion": "$LATEST"
}
{
    "events": [
        {
            "timestamp": 1559763003171,
            "message": "START RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf Version:
 $LATEST\n",
            "ingestionTime": 1559763003309
        },
        {
            "timestamp": 1559763003173,
            "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tENVIRONMENT VARIABLES\r{\r  \"AWS_LAMBDA_FUNCTION_VERSION\": \"$LATEST\",
\r ...",
```

```
            "ingestionTime": 1559763018353
        },
        {
            "timestamp": 1559763003173,
            "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tEVENT\r{\r  \"key\": \"value\"\r}\n",
            "ingestionTime": 1559763018353
        },
        {
            "timestamp": 1559763003218,
            "message": "END RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf\n",
            "ingestionTime": 1559763018353
        },
        {
            "timestamp": 1559763003218,
            "message": "REPORT RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tDuration: 26.73 ms\tBilled Duration: 27 ms \tMemory Size: 128 MB\tMax Memory Used: 75
 MB\t\n",
            "ingestionTime": 1559763018353
        }
    ],
    "nextForwardToken": "f/34783877304859518393868359594929986069206639495374241795",
    "nextBackwardToken": "b/34783877303811383369537420289090800615709599058929582080"
}
```


Suppression de journaux

Les groupes de journaux ne sont pas supprimés automatiquement quand vous supprimez une fonction. Pour éviter de stocker des journaux indéfiniment, supprimez le groupe de journaux ou configurez une période de conservation à l'issue de laquelle les journaux sont supprimés automatiquement.

Exemple de code de journalisation

Le GitHub référentiel de ce guide inclut des exemples d'applications illustrant l'utilisation de différentes configurations de journalisation. Chaque exemple d'application inclut des scripts pour faciliter le déploiement et le nettoyage, un AWS SAM modèle et des ressources de support.

Exemples d'applications Lambda en Java

- example-java — Une fonction d'événement Java qui montre comment utiliser Lambda pour traiter les commandes. Cette fonction montre comment définir et désérialiser un objet d'événement d'entrée personnalisé, utiliser le AWS SDK et enregistrer les sorties.

- java-basic – Ensemble de fonctions Java minimales avec des tests unitaires et une configuration de journalisation variable.
- java events – Ensemble de fonctions Java contenant du code squelette permettant de gérer les événements de divers services tels qu'Amazon API Gateway, Amazon SQS et Amazon Kinesis. Ces fonctions utilisent la dernière version (3.0.0 et ultérieure) de la bibliothèque aws-lambda-java-events. Ces exemples ne nécessitent pas le AWS SDK en tant que dépendance.
- s3-java – Fonction Java qui traite les événements de notification d'Amazon S3 et utilise la bibliothèque de classes Java (JCL) pour créer des miniatures à partir de fichiers d'image chargés.
- layer-java : fonction Java qui illustre comment utiliser une couche Lambda pour empaqueter les dépendances séparément du code de votre fonction principale.

L'exemple `java-basic` d'application présente une configuration de journalisation minimale qui prend en charge les tests de journalisation. Le code du gestionnaire utilise l'enregistreur `LambdaLogger` fourni par l'objet de contexte. Pour les tests, l'application utilise une classe `TestLogger` personnalisée qui implémente l'interface `LambdaLogger` avec un logger Log4j2. Il utilise le SLF4J comme façade pour assurer la compatibilité avec le SDK. AWS Les bibliothèques de journalisation sont exclues de la sortie de build pour limiter la taille du package de déploiement.

Instrumentation du code Java dans AWS Lambda

Lambda s'intègre pour vous aider AWS X-Ray à suivre, à déboguer et à optimiser les applications Lambda. Vous pouvez l'utiliser X-Ray pour suivre une demande lorsqu'elle parcourt les ressources de votre application, ce qui peut inclure des fonctions Lambda et AWS d'autres services.

Pour envoyer des données de suivi à X-Ray, vous pouvez utiliser l'une des deux bibliothèques du SDK :

- AWS Distro for OpenTelemetry (ADOT) — Une distribution sécurisée, prête pour la production et prise AWS en charge du SDK (OTel). OpenTelemetry
- Kit SDK AWS X-Ray pour Java— Un SDK pour générer et envoyer des données de trace à X-Ray.
- Powertools for AWS Lambda (Java) — Une boîte à outils pour les développeurs permettant de mettre en œuvre les meilleures pratiques sans serveur et d'accroître la rapidité des développeurs.

Chacun des SDK propose des moyens d'envoyer vos données de télémétrie au service. X-Ray Vous pouvez ensuite les utiliser X-Ray pour afficher, filtrer et obtenir des informations sur les indicateurs de performance de votre application afin d'identifier les problèmes et les opportunités d'optimisation.

> **Important**
>
> Les X-Ray et Powertools for AWS Lambda SDK font partie d'une solution d'instrumentation étroitement intégrée proposée par. AWS Les couches ADOT Lambda font partie d'une norme industrielle pour l'instrumentation de traçage qui collecte plus de données en général, mais qui peut ne pas convenir à tous les cas d'utilisation. Vous pouvez implémenter le suivi de bout en bout à l' X-Ray aide de l'une ou l'autre solution. Pour en savoir plus sur le choix entre les deux, voir Choisir entre la AWS distribution pour Open Telemetry et les SDK. X-Ray

Sections

- Utilisation de Powertools pour AWS Lambda (Java) et AWS SAM pour le traçage
- Utilisation de Powertools pour AWS Lambda (Java) et le AWS CDK pour le traçage
- Utilisation d'ADOT pour instrumenter vos fonctions Java
- Utiliser le X-Ray SDK pour instrumenter vos fonctions Java
- Activation du suivi avec la console Lambda
- Activation du suivi avec l'API Lambda

- Activation du traçage avec CloudFormation
- Interprétation et X-Ray traçage
- Stockage des dépendances d'exécution dans une couche (X-Ray SDK)
- X-Ray suivi dans des exemples d'applications (X-Ray SDK)

Utilisation de Powertools pour AWS Lambda (Java) et AWS SAM pour le traçage

Suivez les étapes ci-dessous pour télécharger, créer et déployer un exemple d'application Java Hello World avec des modules Powertools for AWS Lambda (Java) intégrés à l'aide du AWS SAM. Cette application met en œuvre un backend API de base et utilise Powertools pour émettre des journaux, des métriques et des traces. Il se compose d'un point de terminaison Amazon API Gateway et d'une fonction d'événement Lambda. Lorsque vous envoyez une requête GET au point de terminaison API Gateway, la fonction Lambda appelle, envoie des journaux et des métriques au format métrique intégré à CloudWatch, et envoie des traces à. AWS X-Ray La fonction renvoie un message `hello world`.

Conditions préalables

Pour exécuter la procédure indiquée dans cette section, vous devez satisfaire aux exigences suivantes :

- Java 11 ou version ultérieure
- AWS CLI version 2
- AWS SAM CLI version 1.75 ou ultérieure. Si vous disposez d'une ancienne version de la AWS SAM CLI, consultez la section Mise à niveau de la AWS SAM CLI.

Déployer un échantillon AWS SAM vigie

1. Initialisez l'application à l'aide du modèle Hello World Java.

```
sam init --app-template hello-world-powertools-java --name sam-app --package-type
 Zip --runtime java11 --no-tracing
```

2. Créez l'application.

```
cd sam-app && sam build
```

3. Déployez l'application.

```
sam deploy --guided
```

4. Suivez les invites à l'écran. Appuyez sur `Enter` pour accepter les options par défaut fournies dans l'expérience interactive.

> **Note**
>
> Car l'autorisation n'a HelloWorldFunction peut-être pas été définie, est-ce que ça va ? , assurez-vous de participery.

5. Obtenez l'URL de l'application déployée :

```
aws cloudformation describe-stacks --stack-name sam-app --query
 'Stacks[0].Outputs[?OutputKey==`HelloWorldApi`].OutputValue' --output text
```

6. Invoquez le point de terminaison de l'API :

```
curl -X GET <URL_FROM_PREVIOUS_STEP>
```

En cas de succès, vous obtiendrez cette réponse :

```
{"message":"hello world"}
```

7. Pour obtenir les traces de la fonction, exécutez sam traces.

```
sam traces
```

La sortie de la trace ressemble à ceci :

```
New XRay Service Graph
  Start time: 2025-02-03 14:31:48+01:00
  End time: 2025-02-03 14:31:48+01:00
  Reference Id: 0 - (Root) AWS::Lambda - sam-app-HelloWorldFunction-y9Iu1FLJJBGD -
 Edges: []
   Summary_statistics:
     - total requests: 1
     - ok count(2XX): 1
     - error count(4XX): 0
     - fault count(5XX): 0
```

```
    - total response time: 5.587
  Reference Id: 1 - client - sam-app-HelloWorldFunction-y9Iu1FLJJBGD - Edges: [0]
   Summary_statistics:
     - total requests: 0
     - ok count(2XX): 0
     - error count(4XX): 0
     - fault count(5XX): 0
     - total response time: 0

XRay Event [revision 3] at (2025-02-03T14:31:48.500000) with id
 (1-63dd0cc4-3c869dec72a586875da39777) and duration (5.603s)
 - 5.587s - sam-app-HelloWorldFunction-y9Iu1FLJJBGD [HTTP: 200]
 - 4.053s - sam-app-HelloWorldFunction-y9Iu1FLJJBGD
   - 1.181s - Initialization
   - 4.037s - Invocation
     - 1.981s - ## handleRequest
       - 1.840s - ## getPageContents
   - 0.000s - Overhead
```

8. Il s’agit d’un point de terminaison d’API public accessible par Internet. Nous vous recommandons de supprimer le point de terminaison après un test.

```
sam delete
```

Utilisation de Powertools pour AWS Lambda (Java) et le AWS CDK pour le traçage

Suivez les étapes ci-dessous pour télécharger, créer et déployer un exemple d'application Java Hello World avec des modules Powertools for AWS Lambda (Java) intégrés à l'aide du AWS CDK. Cette application met en œuvre un backend API de base et utilise Powertools pour émettre des journaux, des métriques et des traces. Il se compose d'un point de terminaison Amazon API Gateway et d'une fonction d'événement Lambda. Lorsque vous envoyez une requête GET au point de terminaison API Gateway, la fonction Lambda appelle, envoie des journaux et des métriques au format métrique intégré à CloudWatch, et envoie des traces à. AWS X-Ray La fonction renvoie un message hello world.

Conditions préalables

Pour exécuter la procédure indiquée dans cette section, vous devez satisfaire aux exigences suivantes :

- Java 11 ou version ultérieure

- AWS CLI version 2
- AWS CDK version 2
- AWS SAM CLI version 1.75 ou ultérieure. Si vous disposez d'une ancienne version de la AWS SAM CLI, consultez la section Mise à niveau de la AWS SAM CLI.

Déployer un échantillon AWS CDK vigie

1. Créez un répertoire de projets pour votre nouvelle application.

```
mkdir hello-world
cd hello-world
```

2. Initialisez l'application.

```
cdk init app --language java
```

3. Créez un projet Maven avec la commande suivante :

```
mkdir app
cd app
mvn archetype:generate -DgroupId=helloworld -DartifactId=Function -
DarchetypeArtifactId=maven-archetype-quickstart -DinteractiveMode=false
```

4. Ouvrez `pom.xml` dans le répertoire `hello-world\app\Function` et remplacez le code existant par le code suivant qui inclut les dépendances et les plugins Maven pour Powertools.

```
<project xmlns="http://maven.apache.org/POM/4.0.0" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://maven.apache.org/POM/4.0.0 http://maven.apache.org/
maven-v4_0_0.xsd">
  <modelVersion>4.0.0</modelVersion>
  <groupId>helloworld</groupId>
  <artifactId>Function</artifactId>
  <packaging>jar</packaging>
  <version>1.0-SNAPSHOT</version>
  <name>Function</name>
  <url>http://maven.apache.org</url>
<properties>
    <maven.compiler.source>11</maven.compiler.source>
    <maven.compiler.target>11</maven.compiler.target>
    <log4j.version>2.17.2</log4j.version>
```

```
</properties>
    <dependencies>
        <dependency>
            <groupId>junit</groupId>
            <artifactId>junit</artifactId>
            <version>3.8.1</version>
            <scope>test</scope>
        </dependency>
        <dependency>
            <groupId>software.amazon.lambda</groupId>
            <artifactId>powertools-tracing</artifactId>
            <version>1.3.0</version>
        </dependency>
        <dependency>
            <groupId>software.amazon.lambda</groupId>
            <artifactId>powertools-metrics</artifactId>
            <version>1.3.0</version>
        </dependency>
        <dependency>
            <groupId>software.amazon.lambda</groupId>
            <artifactId>powertools-logging</artifactId>
            <version>1.3.0</version>
        </dependency>
        <dependency>
            <groupId>com.amazonaws</groupId>
            <artifactId>aws-lambda-java-core</artifactId>
            <version>1.2.2</version>
        </dependency>
        <dependency>
            <groupId>com.amazonaws</groupId>
            <artifactId>aws-lambda-java-events</artifactId>
            <version>3.11.1</version>
        </dependency>
  </dependencies>
<build>
    <plugins>
        <plugin>
            <groupId>org.codehaus.mojo</groupId>
            <artifactId>aspectj-maven-plugin</artifactId>
            <version>1.14.0</version>
            <configuration>
                <source>${maven.compiler.source}</source>
                <target>${maven.compiler.target}</target>
                <complianceLevel>${maven.compiler.target}</complianceLevel>
```

```
                <aspectLibraries>
                    <aspectLibrary>
                        <groupId>software.amazon.lambda</groupId>
                        <artifactId>powertools-tracing</artifactId>
                    </aspectLibrary>
                    <aspectLibrary>
                        <groupId>software.amazon.lambda</groupId>
                        <artifactId>powertools-metrics</artifactId>
                    </aspectLibrary>
                    <aspectLibrary>
                        <groupId>software.amazon.lambda</groupId>
                        <artifactId>powertools-logging</artifactId>
                    </aspectLibrary>
                </aspectLibraries>
            </configuration>
            <executions>
                <execution>
                    <goals>
                        <goal>compile</goal>
                    </goals>
                </execution>
            </executions>
        </plugin>
        <plugin>
                <groupId>org.apache.maven.plugins</groupId>
                <artifactId>maven-shade-plugin</artifactId>
                <version>3.4.1</version>
                <executions>
                    <execution>
                        <phase>package</phase>
                        <goals>
                            <goal>shade</goal>
                        </goals>
                        <configuration>
                            <transformers>
                                <transformer

 implementation="com.github.edwgiz.maven_shade_plugin.log4j2_cache_transformer.PluginsCache
                                </transformer>
                            </transformers>
                            <createDependencyReducedPom>false</
createDependencyReducedPom>
                            <finalName>function</finalName>
```

```
                        </configuration>
                    </execution>
                </executions>
                <dependencies>
                    <dependency>
                        <groupId>com.github.edwgiz</groupId>
                        <artifactId>maven-shade-plugin.log4j2-cachefile-
transformer</artifactId>
                        <version>2.15</version>
                    </dependency>
                </dependencies>
        </plugin>
    </plugins>
</build>
</project>
```

5. Créez le répertoire `hello-world\app\src\main\resource` et créez `log4j.xml` pour la configuration du journal.

```
mkdir -p src/main/resource
cd src/main/resource
touch log4j.xml
```

6. Ouvrez `log4j.xml` et ajoutez le code suivant.

```
<?xml version="1.0" encoding="UTF-8"?>
<Configuration>
    <Appenders>
        <Console name="JsonAppender" target="SYSTEM_OUT">
            <JsonTemplateLayout
 eventTemplateUri="classpath:LambdaJsonLayout.json" />
        </Console>
    </Appenders>
    <Loggers>
        <Logger name="JsonLogger" level="INFO" additivity="false">
            <AppenderRef ref="JsonAppender"/>
        </Logger>
        <Root level="info">
            <AppenderRef ref="JsonAppender"/>
        </Root>
    </Loggers>
</Configuration>
```

7. Ouvrez `App.java` à partir du répertoire `hello-world\app\Function\src\main\java\helloworld` et remplacez le code existant par le code suivant. Il s'agit du code de la fonction Lambda.

```
package helloworld;

import java.io.BufferedReader;
import java.io.IOException;
import java.io.InputStreamReader;
import java.net.URL;
import java.util.HashMap;
import java.util.Map;
import java.util.stream.Collectors;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.APIGatewayProxyRequestEvent;
import com.amazonaws.services.lambda.runtime.events.APIGatewayProxyResponseEvent;
import org.apache.logging.log4j.LogManager;
import org.apache.logging.log4j.Logger;
import software.amazon.lambda.powertools.logging.Logging;
import software.amazon.lambda.powertools.metrics.Metrics;
import software.amazon.lambda.powertools.tracing.CaptureMode;
import software.amazon.lambda.powertools.tracing.Tracing;

import static software.amazon.lambda.powertools.tracing.CaptureMode.*;

/**
 * Handler for requests to Lambda function.
 */
public class App implements RequestHandler<APIGatewayProxyRequestEvent,
 APIGatewayProxyResponseEvent> {
    Logger log = LogManager.getLogger(App.class);


    @Logging(logEvent = true)
    @Tracing(captureMode = DISABLED)
    @Metrics(captureColdStart = true)
    public APIGatewayProxyResponseEvent handleRequest(final
 APIGatewayProxyRequestEvent input, final Context context) {
        Map<String, String> headers = new HashMap<>();
        headers.put("Content-Type", "application/json");
        headers.put("X-Custom-Header", "application/json");
```

```
        APIGatewayProxyResponseEvent response = new APIGatewayProxyResponseEvent()
                .withHeaders(headers);
        try {
            final String pageContents = this.getPageContents("https://
checkip.amazonaws.com");
            String output = String.format("{ \"message\": \"hello world\",
 \"location\": \"%s\" }", pageContents);

            return response
                    .withStatusCode(200)
                    .withBody(output);
        } catch (IOException e) {
            return response
                    .withBody("{}")
                    .withStatusCode(500);
        }
    }
    @Tracing(namespace = "getPageContents")
    private String getPageContents(String address) throws IOException {
        log.info("Retrieving {}", address);
        URL url = new URL(address);
        try (BufferedReader br = new BufferedReader(new
 InputStreamReader(url.openStream()))) {
            return br.lines().collect(Collectors.joining(System.lineSeparator()));
        }
    }
}
```

8. Ouvrez `HelloWorldStack.java` à partir du répertoire `hello-world\src\main\java\com\myorg` et remplacez le code existant par le code suivant. Ce code utilise le constructeur Lambda et le constructeur ApiGatewayv 2 pour créer une API REST et une fonction d'événement Lambda.

```
package com.myorg;

import software.amazon.awscdk.*;
import software.amazon.awscdk.services.apigatewayv2.alpha.*;
import
 software.amazon.awscdk.services.apigatewayv2.integrations.alpha.HttpLambdaIntegration;
import
 software.amazon.awscdk.services.apigatewayv2.integrations.alpha.HttpLambdaIntegrationProps
import software.amazon.awscdk.services.lambda.Code;
```

```
import software.amazon.awscdk.services.lambda.Function;
import software.amazon.awscdk.services.lambda.FunctionProps;
import software.amazon.awscdk.services.lambda.Runtime;
import software.amazon.awscdk.services.lambda.Tracing;
import software.amazon.awscdk.services.logs.RetentionDays;
import software.amazon.awscdk.services.s3.assets.AssetOptions;
import software.constructs.Construct;

import java.util.Arrays;
import java.util.List;

import static java.util.Collections.singletonList;
import static software.amazon.awscdk.BundlingOutput.ARCHIVED;

public class HelloWorldStack extends Stack {
    public HelloWorldStack(final Construct scope, final String id) {
        this(scope, id, null);
    }

    public HelloWorldStack(final Construct scope, final String id, final StackProps
 props) {
        super(scope, id, props);

        List<String> functionPackagingInstructions = Arrays.asList(
                "/bin/sh",
                "-c",
                "cd Function " +
                        "&& mvn clean install " +
                        "&& cp /asset-input/Function/target/function.jar /asset-
output/"
        );
        BundlingOptions.Builder builderOptions = BundlingOptions.builder()
                .command(functionPackagingInstructions)
                .image(Runtime.JAVA_11.getBundlingImage())
                .volumes(singletonList(
                        // Mount local .m2 repo to avoid download all the
 dependencies again inside the container
                        DockerVolume.builder()
                                .hostPath(System.getProperty("user.home") +
 "/.m2/")
                                .containerPath("/root/.m2/")
                                .build()
                ))
                .user("root")
```

```
                .outputType(ARCHIVED);

        Function function = new Function(this, "Function", FunctionProps.builder()
                .runtime(Runtime.JAVA_11)
                .code(Code.fromAsset("app", AssetOptions.builder()
                        .bundling(builderOptions
                                .command(functionPackagingInstructions)
                                .build())
                        .build()))
                .handler("helloworld.App::handleRequest")
                .memorySize(1024)
                .tracing(Tracing.ACTIVE)
                .timeout(Duration.seconds(10))
                .logRetention(RetentionDays.ONE_WEEK)
                .build());

        HttpApi httpApi = new HttpApi(this, "sample-api", HttpApiProps.builder()
                .apiName("sample-api")
                .build());

        httpApi.addRoutes(AddRoutesOptions.builder()
                .path("/")
                .methods(singletonList(HttpMethod.GET))
                .integration(new HttpLambdaIntegration("function", function,
 HttpLambdaIntegrationProps.builder()
                        .payloadFormatVersion(PayloadFormatVersion.VERSION_2_0)
                        .build()))
                .build());

        new CfnOutput(this, "HttpApi", CfnOutputProps.builder()
                .description("Url for Http Api")
                .value(httpApi.getApiEndpoint())
                .build());
    }
}
```

9. Ouvrez `pom.xml` à partir du répertoire `hello-world` et remplacez le code existant par le code suivant.

```
<?xml version="1.0" encoding="UTF-8"?>
<project xsi:schemaLocation="http://maven.apache.org/POM/4.0.0 http://
maven.apache.org/xsd/maven-4.0.0.xsd"
```

```
         xmlns="http://maven.apache.org/POM/4.0.0" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">
    <modelVersion>4.0.0</modelVersion>

    <groupId>com.myorg</groupId>
    <artifactId>hello-world</artifactId>
    <version>0.1</version>

    <properties>
        <project.build.sourceEncoding>UTF-8</project.build.sourceEncoding>
        <cdk.version>2.70.0</cdk.version>
        <constructs.version>[10.0.0,11.0.0)</constructs.version>
        <junit.version>5.7.1</junit.version>
    </properties>

    <build>
        <plugins>
            <plugin>
                <groupId>org.apache.maven.plugins</groupId>
                <artifactId>maven-compiler-plugin</artifactId>
                <version>3.8.1</version>
                <configuration>
                    <source>1.8</source>
                    <target>1.8</target>
                </configuration>
            </plugin>

            <plugin>
                <groupId>org.codehaus.mojo</groupId>
                <artifactId>exec-maven-plugin</artifactId>
                <version>3.0.0</version>
                <configuration>
                    <mainClass>com.myorg.HelloWorldApp</mainClass>
                </configuration>
            </plugin>
        </plugins>
    </build>

    <dependencies>
        <!-- AWS Cloud Development Kit -->
        <dependency>
            <groupId>software.amazon.awscdk</groupId>
            <artifactId>aws-cdk-lib</artifactId>
            <version>${cdk.version}</version>
```

```
        </dependency>
        <dependency>
            <groupId>software.constructs</groupId>
            <artifactId>constructs</artifactId>
            <version>${constructs.version}</version>
        </dependency>
        <dependency>
          <groupId>org.junit.jupiter</groupId>
          <artifactId>junit-jupiter</artifactId>
          <version>${junit.version}</version>
          <scope>test</scope>
        </dependency>
        <dependency>
            <groupId>software.amazon.awscdk</groupId>
            <artifactId>apigatewayv2-alpha</artifactId>
            <version>${cdk.version}-alpha.0</version>
        </dependency>
        <dependency>
            <groupId>software.amazon.awscdk</groupId>
            <artifactId>apigatewayv2-integrations-alpha</artifactId>
            <version>${cdk.version}-alpha.0</version>
        </dependency>
    </dependencies>
</project>
```

10. Vérifiez que vous êtes dans le `hello-world` répertoire et déployez votre application.

```
cdk deploy
```

11. Obtenez l'URL de l'application déployée :

```
aws cloudformation describe-stacks --stack-name HelloWorldStack --query
 'Stacks[0].Outputs[?OutputKey==`HttpApi`].OutputValue' --output text
```

12. Invoquez le point de terminaison de l'API :

```
curl -X GET <URL_FROM_PREVIOUS_STEP>
```

    En cas de succès, vous obtiendrez cette réponse :

```
{"message":"hello world"}
```

13. Pour obtenir les traces de la fonction, exécutez sam traces.

```
sam traces
```

La sortie de la trace ressemble à ceci :

```
New XRay Service Graph
  Start time: 2025-02-03 14:59:50+00:00
  End time: 2025-02-03 14:59:50+00:00
  Reference Id: 0 - (Root) AWS::Lambda - sam-app-HelloWorldFunction-YBg8yfYtOc9j -
 Edges: [1]
   Summary_statistics:
     - total requests: 1
     - ok count(2XX): 1
     - error count(4XX): 0
     - fault count(5XX): 0
     - total response time: 0.924
  Reference Id: 1 - AWS::Lambda::Function - sam-app-HelloWorldFunction-YBg8yfYtOc9j
 - Edges: []
   Summary_statistics:
     - total requests: 1
     - ok count(2XX): 1
     - error count(4XX): 0
     - fault count(5XX): 0
     - total response time: 0.016
  Reference Id: 2 - client - sam-app-HelloWorldFunction-YBg8yfYtOc9j - Edges: [0]
   Summary_statistics:
     - total requests: 0
     - ok count(2XX): 0
     - error count(4XX): 0
     - fault count(5XX): 0
     - total response time: 0

XRay Event [revision 1] at (2025-02-03T14:59:50.204000) with id
 (1-63dd2166-434a12c22e1307ff2114f299) and duration (0.924s)
 - 0.924s - sam-app-HelloWorldFunction-YBg8yfYtOc9j [HTTP: 200]
 - 0.016s - sam-app-HelloWorldFunction-YBg8yfYtOc9j
   - 0.739s - Initialization
   - 0.016s - Invocation
     - 0.013s - ## lambda_handler
       - 0.000s - ## app.hello
   - 0.000s - Overhead
```

14. Il s’agit d’un point de terminaison d’API public accessible par Internet. Nous vous recommandons de supprimer le point de terminaison après un test.

```
cdk destroy
```

Utilisation d'ADOT pour instrumenter vos fonctions Java

ADOT fournit des couches Lambda entièrement gérées qui regroupent tout ce dont vous avez besoin pour collecter des données de télémétrie à l'aide du kit SDK OTel. En consommant cette couche, vous pouvez instrumenter vos fonctions Lambda sans avoir à modifier le code de fonction. Vous pouvez également configurer votre couche pour effectuer une initialisation personnalisée d’OTel. Pour de plus amples informations, veuillez consulter Configuration personnalisée pour ADOT Collector sur Lambda dans la documentation ADOT.

Pour les environnements d'exécution Java, vous pouvez choisir entre deux couches à consommer :

- AWS couche Lambda gérée pour ADOT Java (Auto-instrumentation Agent) : cette couche transforme automatiquement le code de votre fonction au démarrage pour collecter des données de suivi. Pour obtenir des instructions détaillées sur la façon d'utiliser cette couche avec l'agent Java ADOT, consultez AWS Distro for Lambda OpenTelemetry Support for Java (Auto-instrumentation Agent) dans la documentation ADOT.
- AWS couche Lambda gérée pour ADOT Java — Cette couche fournit également une instrumentation intégrée pour les fonctions Lambda, mais elle nécessite quelques modifications de code manuelles pour initialiser le SDK OTel. Pour obtenir des instructions détaillées sur la façon de consommer cette couche, consultez AWS Distro for OpenTelemetry Lambda Support for Java dans la documentation ADOT.

Pour obtenir des instructions sur la conversion des événements de l'API de télémétrie Lambda en spans, consultez. OpenTelemetry the section called “Conversion d’événements en OTel Spans”

Utiliser le X-Ray SDK pour instrumenter vos fonctions Java

Pour enregistrer les données relatives aux appels que votre fonction effectue vers d'autres ressources et services de votre application, vous pouvez ajouter le X-Ray SDK for Java à votre configuration de compilation. L'exemple suivant montre une configuration de build Gradle qui inclut les bibliothèques qui activent l'instrumentation automatique des AWS SDK for Java 2.x clients.

Example build.gradle — Suivi des dépendances

```
dependencies {
    implementation platform('software.amazon.awssdk:bom:2.16.1')
    implementation platform('com.amazonaws:aws-xray-recorder-sdk-bom:2.11.0')
    ...
    implementation 'com.amazonaws:aws-xray-recorder-sdk-core'
    implementation 'com.amazonaws:aws-xray-recorder-sdk-aws-sdk'
    implementation 'com.amazonaws:aws-xray-recorder-sdk-aws-sdk-v2-instrumentor'
    ...
}
```

Après avoir ajouté les bonnes dépendances et apporté les modifications de code nécessaires, activez le suivi dans la configuration de votre fonction via la console Lambda ou l'API.

Activation du suivi avec la console Lambda

Pour activer le suivi actif de votre fonction d'événement Lambda à l'aide de la console, procédez comme suit :

Pour activer le traçage actif

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez une fonction d'événement.
3. Choisissez Configuration, puis choisissez Outils de surveillance et d’opérations.
4. Dans Outils de surveillance supplémentaires, choisissez Modifier.
5. Sous Signaux CloudWatch d'application et AWS X-Ray sélectionnez Activer les traces de service Lambda.
6. Cliquez sur Enregistrer.

Activation du suivi avec l’API Lambda

Configurez le suivi sur votre fonction Lambda avec le AWS SDK AWS CLI or, utilisez les opérations d'API suivantes :

- UpdateFunctionConfiguration
- GetFunctionConfiguration
- CreateFunction

L'exemple de AWS CLI commande suivant active le suivi actif sur une fonction nommée my-function.

```
aws lambda update-function-configuration --function-name my-function \
--tracing-config Mode=Active
```

Le mode de suivi fait partie de la configuration spécifique de la version lorsque vous publiez une version de votre fonction. Vous ne pouvez pas modifier le mode de suivi sur une version publiée.

Activation du traçage avec CloudFormation

Pour activer le suivi d'une `AWS::Lambda::Function` ressource dans un CloudFormation modèle, utilisez la `TracingConfig` propriété.

Example fonction-inline.yml — Configuration du suivi

```
Resources:
  function:
    Type: AWS::Lambda::Function
    Properties:
      TracingConfig:
        Mode: Active
      ...
```

Pour une `AWS::Serverless::Function` ressource AWS Serverless Application Model (AWS SAM), utilisez la `Tracing` propriété.

Example template.yml — Configuration du suivi

```
Resources:
  function:
    Type: AWS::Serverless::Function
    Properties:
      Tracing: Active
      ...
```

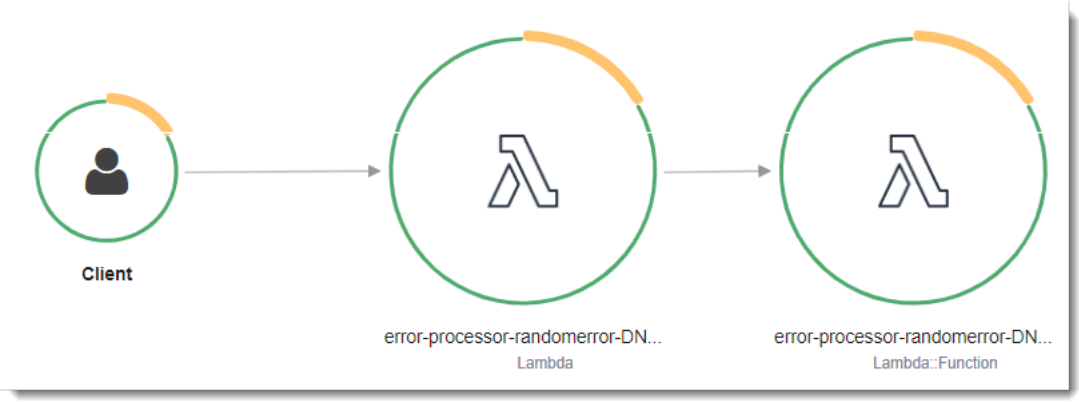
Interprétation et X-Ray traçage

Votre fonction événementielle a besoin d'une autorisation pour télécharger des données de suivi sur X-Ray. Lorsque vous activez le suivi dans la console Lambda, Lambda ajoute les autorisations requises au rôle d'exécution de votre fonction d'événement. Dans le cas contraire, ajoutez la AWSXRayDaemonWriteAccesspolitique au rôle d'exécution.

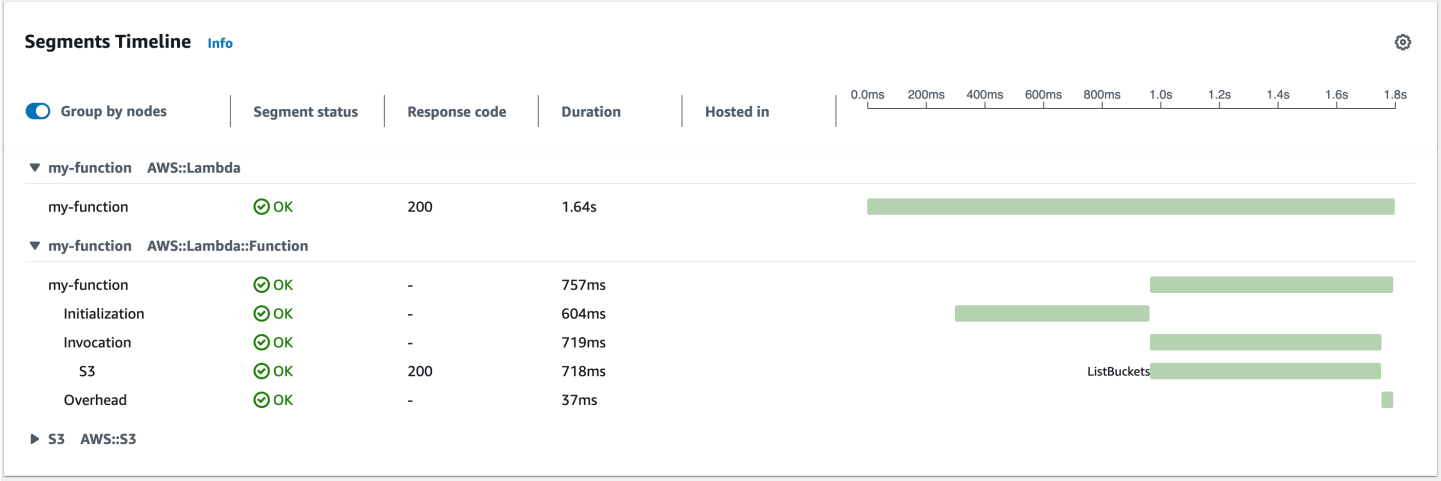
Une fois que vous avez configuré le suivi actif, vous pouvez observer des demandes spécifiques via votre application. Le graphique X-Ray de service affiche des informations sur votre application et tous ses composants. L'exemple suivant montre une application dotée de deux fonctions. La fonction principale traite les événements et renvoie parfois des erreurs. La deuxième fonction située en haut traite les erreurs qui apparaissent dans le groupe de journaux de la première et utilise le AWS SDK pour appeler X-Ray Amazon Simple Storage Service (Amazon S3) et Amazon Logs. CloudWatch

X-Ray ne retrace pas toutes les demandes jusqu'à votre application. X-Ray applique un algorithme d'échantillonnage pour garantir l'efficacité du suivi, tout en fournissant un échantillon représentatif de toutes les demandes. Le taux d'échantillonnage est 1 demande par seconde et 5 % de demandes supplémentaires. Vous ne pouvez pas configurer le taux X-Ray d'échantillonnage pour vos fonctions.

Dans X-Ray, un suivi enregistre des informations relatives à une demande traitée par un ou plusieurs services. Lambda enregistre deux segments par suivi, ce qui a pour effet de créer deux nœuds sur le graphique du service. L'image suivante met en évidence ces deux nœuds :



Le premier nœud sur la gauche représente le service Lambda qui reçoit la demande d'invocation. Le deuxième nœud représente votre fonction Lambda spécifique. L'exemple suivant illustre une trace avec ces deux segments. Les deux sont nommés my-function, mais l'un a pour origine `AWS::Lambda` et l'autre a pour origine `AWS::Lambda::Function`. Si le segment `AWS::Lambda` affiche une erreur, cela signifie que le service Lambda a rencontré un problème. Si le segment `AWS::Lambda::Function` affiche une erreur, cela signifie que votre fonction a rencontré un problème.



Cet exemple développe le segment `AWS::Lambda::Function` pour afficher ses trois sous-segments.

> **Note**
>
> AWS met actuellement en œuvre des modifications du service Lambda. En raison de ces modifications, vous pouvez constater des différences mineures entre la structure et le contenu des messages du journal système et des segments de trace émis par les différentes fonctions d'événement Lambda de votre ordinateur. Compte AWS
> L'exemple de suivi présenté ici illustre le segment de fonction à l'ancienne. Les différences entre les segments à l'ancienne et de style moderne sont décrites dans les paragraphes suivants.
> Ces modifications seront mises en œuvre au cours des prochaines semaines, et toutes les fonctions, Régions AWS sauf en Chine et dans les GovCloud régions, seront transférées pour utiliser le nouveau format des messages de journal et des segments de trace.

Le segment de fonction à l'ancienne contient les sous-segments suivants :

- Initialization (Initialisation) : représente le temps passé à charger votre fonction et à exécuter le code d'initialisation. Ce sous-segment apparaît pour le premier événement traité par chaque instance de votre fonction.
- Invocation – Représente le temps passé à exécuter votre code de gestionnaire.
- Overhead (Travail supplémentaire) – Représente le temps que le fichier d'exécution Lambda passe à se préparer à gérer l'événement suivant.

Le segment de fonction de style moderne ne contient pas de sous-segment `Invocation`. À la place, les sous-segments du client sont directement rattachés au segment de fonction. Pour plus d'informations sur la structure des segments de fonction à l'ancienne et de style moderne, consultez the section called "Comprendre les X-Ray traces".

> **Note**
>
> Les fonctions SnapStart incluent également un sous-segment `Restore`. Le sous-segment `Restore` indique le temps nécessaire à Lambda pour restaurer un instantané, charger l'exécution et exécuter les éventuels hooks d'exécution après restauration. Le processus de restauration des instantanés peut inclure du temps consacré à des activités en dehors de la MicroVM. Cette heure est indiquée dans le sous-segment `Restore`. Le temps passé en dehors de la microVM pour restaurer un instantané ne vous est pas facturé.

Vous pouvez également utiliser des clients HTTP, enregistrer des requêtes SQL et créer des sous-segments personnalisés avec des annotations et des métadonnées. Pour plus d'informations, consultez Kit SDK AWS X-Ray pour Java dans le Guide du développeur AWS X-Ray .

> **Tarification**
>
> Vous pouvez utiliser le X-Ray suivi gratuitement chaque mois jusqu'à une certaine limite dans le cadre du niveau AWS gratuit. Au-delà de ce seuil, les X-Ray frais de stockage et de récupération des traces sont facturés. Pour en savoir plus, consultez Pricing AWS X-Ray (Tarification).

Stockage des dépendances d'exécution dans une couche (X-Ray SDK)

Si vous utilisez le X-Ray SDK pour instrumenter le code de fonction des clients du AWS SDK, votre package de déploiement peut devenir assez volumineux. Pour éviter de télécharger les dépendances d'exécution chaque fois que vous mettez à jour le code de votre fonction, empaquetez le X-Ray SDK dans une couche Lambda.

L'exemple suivant montre une `AWS::Serverless::LayerVersion` ressource qui stocke le X-Ray SDK AWS SDK pour Java and pour Java.

Example template.yml — Couche de dépendances

```
Resources:
  function:
    Type: AWS::Serverless::Function
    Properties:
      CodeUri: build/distributions/blank-java.zip
      Tracing: Active
      Layers:
        - !Ref libs
      ...
  libs:
    Type: AWS::Serverless::LayerVersion
    Properties:
      LayerName: blank-java-lib
      Description: Dependencies for the blank-java sample app.
      ContentUri: build/blank-java-lib.zip
      CompatibleRuntimes:
        - java25
```

Avec cette configuration, vous ne mettez à jour les fichiers de couche de bibliothèque que si vous modifiez vos dépendances d’exécution. Étant donné que le package de déploiement de la fonction contient uniquement votre code, cela peut contribuer à réduire les temps de chargement.

La création d'une couche pour les dépendances nécessite des modifications de configuration pour générer l'archive de couches avant le déploiement. Pour un exemple pratique, consultez l'exemple d'application java-basic sur. GitHub

X-Ray suivi dans des exemples d'applications (X-Ray SDK)

Le GitHub référentiel de ce guide inclut des exemples d'applications illustrant l'utilisation du X-Ray traçage. Chaque exemple d'application inclut des scripts pour faciliter le déploiement et le nettoyage, un AWS SAM modèle et des ressources de support.

Exemples d’applications Lambda en Java

- example-java — Une fonction d'événement Java qui montre comment utiliser Lambda pour traiter les commandes. Cette fonction montre comment définir et désérialiser un objet d'événement d'entrée personnalisé, utiliser le AWS SDK et enregistrer les sorties.
- java-basic – Ensemble de fonctions Java minimales avec des tests unitaires et une configuration de journalisation variable.
- java events – Ensemble de fonctions Java contenant du code squelette permettant de gérer les événements de divers services tels qu’Amazon API Gateway, Amazon SQS et Amazon Kinesis. Ces fonctions utilisent la dernière version (3.0.0 et ultérieure) de la bibliothèque aws-lambda-java-events. Ces exemples ne nécessitent pas le AWS SDK en tant que dépendance.
- s3-java – Fonction Java qui traite les événements de notification d’Amazon S3 et utilise la bibliothèque de classes Java (JCL) pour créer des miniatures à partir de fichiers d’image chargés.
- layer-java : fonction Java qui illustre comment utiliser une couche Lambda pour empaqueter les dépendances séparément du code de votre fonction principale.

Tous les exemples d'applications ont un suivi actif activé pour les fonctions Lambda. Par exemple, l'`s3-java`application montre l'instrumentation automatique des AWS SDK for Java 2.x clients, la gestion des segments pour les tests, les sous-segments personnalisés et l'utilisation de couches Lambda pour stocker les dépendances d'exécution.

Exemples d'applications Java pour AWS Lambda

Le GitHub référentiel de ce guide fournit des exemples d'applications illustrant l'utilisation de Java dans AWS Lambda. Chaque exemple d'application inclut des scripts pour faciliter le déploiement et le nettoyage, un CloudFormation modèle et des ressources de support.

Exemples d’applications Lambda en Java

- example-java — Une fonction d'événement Java qui montre comment utiliser Lambda pour traiter les commandes. Cette fonction montre comment définir et désérialiser un objet d'événement d'entrée personnalisé, utiliser le AWS SDK et enregistrer les sorties.
- java-basic – Ensemble de fonctions Java minimales avec des tests unitaires et une configuration de journalisation variable.
- java events – Ensemble de fonctions Java contenant du code squelette permettant de gérer les événements de divers services tels qu’Amazon API Gateway, Amazon SQS et Amazon Kinesis. Ces fonctions utilisent la dernière version (3.0.0 et ultérieure) de la bibliothèque aws-lambda-java-events. Ces exemples ne nécessitent pas le AWS SDK en tant que dépendance.
- s3-java – Fonction Java qui traite les événements de notification d’Amazon S3 et utilise la bibliothèque de classes Java (JCL) pour créer des miniatures à partir de fichiers d’image chargés.
- layer-java : fonction Java qui illustre comment utiliser une couche Lambda pour empaqueter les dépendances séparément du code de votre fonction principale.

Exécution de cadres Java populaires sur Lambda

- spring-cloud-function-samples — Exemple tiré de Spring qui montre comment utiliser le framework Spring Cloud Function pour créer des fonctions d'événement Lambda. AWS
- Démo de l'application Spring Boot sans serveur : exemple qui montre comment configurer une application Spring Boot typique dans un environnement d'exécution Java géré avec ou sans SnapStart, ou en tant qu'image native de GraalVM avec un environnement d'exécution personnalisé.
- Démonstration de l'application Micronaut sans serveur — Un exemple qui montre comment utiliser Micronaut dans un environnement d'exécution Java géré avec et sans SnapStart, ou en tant qu'image native de GraalVM avec un environnement d'exécution personnalisé. Pour en savoir plus, consultez les Micronaut/Lambda guides.
- Démo de l'application Quarkus sans serveur — Un exemple qui montre comment utiliser Quarkus dans un environnement d'exécution Java géré avec et sans SnapStart, ou en tant qu'image native

de GraalVM avec un environnement d'exécution personnalisé. Pour en savoir plus, consultez le Quarkus/Lambda guide et le Quarkus/SnapStart guide.

Si vous ne connaissez pas encore les fonctions d'événement Lambda en Java, commencez par les `java-basic` exemples. Pour démarrer avec les sources d'événement Lambda, consultez les exemples `java-events`. Ces deux ensembles d'exemples montrent l'utilisation des bibliothèques Java, des variables d'environnement, du SDK et du AWS SDK de Lambda. AWS X-Ray Ces exemples nécessitent une configuration minimale et peuvent être déployé à partir de la ligne de commande en moins d'une minute.

Création de fonctions événementielles Lambda avec Go

Go est implémenté différemment des autres exécutions gérées. Go se compilant nativement en un binaire exécutable, il n'a pas besoin d'un environnement d'exécution dédié au langage. Utilisez un OS-only exécution (les `provided` famille d'exécution) pour déployer Go Event Functions sur Lambda.

Pour plus d'informations sur l'utilisation des couches avec Go, voir the section called "Layers".

Rubriques

- Prise en charge de l'exécution Go
- Outils et bibliothèques
- Définir les gestionnaires de fonctions d'événement Lambda dans Go
- Utilisation de l'objet de contexte Lambda pour récupérer les informations de la fonction Go Event
- Déployez les fonctions d'événement Go Lambda avec des archives de fichiers .zip
- Déployez les fonctions d'événement Go Lambda avec des images de conteneur
- Utilisation de couches pour les fonctions d'événement Go Lambda
- Enregistrez et surveillez les fonctions des événements Go Lambda
- Instrumentation du code Go AWS Lambda

Prise en charge de l'exécution Go

L'environnement d'exécution géré par Go 1.x pour Lambda est obsolète. Si vous utilisez l'environnement d'exécution Go 1.x, vous devez transférer vos fonctions vers `provided.al2023` ou `provided.al2`. Le `provided.al2023` et `provided.al2` les temps d'exécution offrent

plusieurs avantages par rapport à `go1.x`, y compris la prise en charge de l'architecture arm64 (AWS processeurs Graviton), des fichiers binaires plus petits et des temps d'appel légèrement plus rapides.

Aucune modification du code n'est requise pour cette migration. Les seules modifications requises concernent la façon dont vous créez votre package de déploiement et l'exécution que vous utilisez pour créer votre fonction. Pour plus d'informations, voir Migration AWS Lambda fonctions du Go1.x exécution vers l'environnement d'exécution personnalisé sur Amazon Linux 2 sur le AWS Blog informatique.

Nom	Identifiant	Système d'exploitation	Date d'obsolescence	Créer la fonction de blocage	Mettre à jour la fonction de blocage
OS-only Temps d'exécution	`provided.al2023`	Amazon Linux 2	30 juin 2029	31 juillet 2029	31 août 2029

Outils et bibliothèques

Lambda fournit les outils et bibliothèques suivants pour l'environnement d'exécution Go :

- AWS SDK pour Go v2: L'officiel AWS SDK pour le langage de programmation Go.
- github.com/aws/aws-lambda-go/lambda: L'implémentation du modèle de programmation Lambda pour Go. Ce package est utilisé par AWS Lambda pour invoquer votre gestionnaire.
- github.com/aws/aws-lambda-go/lambdacontext: aides pour accéder aux informations contextuelles depuis le objet de contexte.
- github.com/aws/aws-lambda-go/events: cette bibliothèque fournit des définitions de type pour les intégrations de sources d'événements courantes.
- github.com/aws/aws-lambda-go/cmd/build-lambda-zip: Cet outil peut être utilisé pour créer une archive de fichiers .zip sous Windows.

Pour plus d'informations, voir aws-Lambda Go sur GitHub.

Lambda fournit les exemples d'applications suivants pour l'environnement d'exécution Go :

Exemples d’applications Lambda en Go

- go-al2 – Une fonction Hello World qui renvoie l’adresse IP publique. Cette application utilise l’exécution personnalisée `provided.al2`.
- blank-go — Une fonction Go qui montre l'utilisation des bibliothèques Go de Lambda, la journalisation, les variables d'environnement et le AWS SDK. Cette application utilise l’exécution `go1.x`.

Définir les gestionnaires de fonctions d'événement Lambda dans Go

Le gestionnaire de fonctions d'événement Lambda est la méthode de votre code de fonction qui traite les événements. Lorsque votre fonction est invoquée, Lambda exécute la méthode du gestionnaire. Votre fonction s'exécute jusqu'à ce que le gestionnaire renvoie une réponse, se ferme ou expire.

Cette page explique comment utiliser les gestionnaires de fonctions d'événement Lambda dans Go, notamment la configuration du projet, les conventions de dénomination et les meilleures pratiques. Cette page inclut également un exemple de fonction Lambda Go qui collecte des informations relatives à une commande, produit un reçu sous forme de fichier texte et place ce fichier dans un compartiment Amazon Simple Storage Service (Amazon S3). Pour plus d'informations sur le déploiement de votre fonction après l'avoir écrite, consultez the section called "Déploiement d'archives de fichiers .zip" ou the section called "Déploiement d'images de conteneur".

Rubriques

- Configuration de votre projet de gestionnaire Go
- Exemple de code de fonction d'événement Go Lambda
- Convention de nommage du gestionnaire
- Définition et accès à l'objet d'événement d'entrée
- Accès et utilisation de l'objet de contexte Lambda
- Signatures de gestionnaire valides pour les gestionnaires Go
- Utilisation de AWS SDK pour Go v2 dans votre gestionnaire
- Accès aux variables d'environnement
- Utilisation de l'état global
- Meilleures pratiques en matière de code pour les fonctions d'événement Go Lambda

Configuration de votre projet de gestionnaire Go

Une fonction Lambda écrite en Go est créée en tant qu'exécutable Go. Vous pouvez initialiser un projet de fonction Lambda Go de la même manière que vous initialisez n'importe quel autre projet Go à l'aide de la commande suivante : `go mod init`

```
go mod init example-go
```

Ici, `example-go` est le nom du module. Vous pouvez le remplacer par n'importe quelle valeur. Cette commande initialise votre projet et génère le fichier `go.mod` répertoriant les dépendances de votre projet.

Utilisez la commande `go get` pour ajouter des dépendances externes à votre projet. Par exemple, pour toutes les fonctions Lambda de Go, vous devez inclure le github. com/awsgo/lambdapackage / aws-lambda-, qui implémente le modèle de programmation Lambda pour Go. Installez ce package à l'aide de la commande `go get` suivante :

```
go get github.com/aws/aws-lambda-go
```

Le code de votre fonction doit résider dans un fichier Go. Dans l'exemple suivant, nous nommons ce fichier `main.go`. Dans ce fichier, vous implémentez la logique de votre fonction de base dans une méthode de gestion, ainsi que dans une fonction `main()` qui appelle ce gestionnaire.

Exemple de code de fonction d'événement Go Lambda

L'exemple de code de fonction Lambda Go suivant prend en compte les informations relatives à une commande, produit un reçu sous forme de fichier texte et place ce fichier dans un compartiment Amazon S3.

Example Fonction d'événement **`Lambda main.go`**

```
package main

import (
 "context"
 "encoding/json"
 "fmt"
 "log"
 "os"
 "strings"

 "github.com/aws/aws-lambda-go/lambda"
 "github.com/aws/aws-sdk-go-v2/config"
 "github.com/aws/aws-sdk-go-v2/service/s3"
)

type Order struct {
 OrderID string  `json:"order_id"`
 Amount  float64 `json:"amount"`
 Item    string  `json:"item"`
```

```
}

var (
 s3Client *s3.Client
)

func init() {
 // Initialize the S3 client outside of the handler, during the init phase
 cfg, err := config.LoadDefaultConfig(context.TODO())
 if err != nil {
  log.Fatalf("unable to load SDK config, %v", err)
 }

 s3Client = s3.NewFromConfig(cfg)
}

func uploadReceiptToS3(ctx context.Context, bucketName, key, receiptContent string)
 error {
 _, err := s3Client.PutObject(ctx, &s3.PutObjectInput{
  Bucket: &bucketName,
  Key:    &key,
  Body:   strings.NewReader(receiptContent),
 })
 if err != nil {
  log.Printf("Failed to upload receipt to S3: %v", err)
  return err
 }
 return nil
}

func handleRequest(ctx context.Context, event json.RawMessage) error {
 // Parse the input event
 var order Order
 if err := json.Unmarshal(event, &order); err != nil {
  log.Printf("Failed to unmarshal event: %v", err)
  return err
 }

 // Access environment variables
 bucketName := os.Getenv("RECEIPT_BUCKET")
 if bucketName == "" {
  log.Printf("RECEIPT_BUCKET environment variable is not set")
  return fmt.Errorf("missing required environment variable RECEIPT_BUCKET")
 }
```

```
 // Create the receipt content and key destination
 receiptContent := fmt.Sprintf("OrderID: %s\nAmount: $%.2f\nItem: %s",
  order.OrderID, order.Amount, order.Item)
 key := "receipts/" + order.OrderID + ".txt"

 // Upload the receipt to S3 using the helper method
 if err := uploadReceiptToS3(ctx, bucketName, key, receiptContent); err != nil {
  return err
 }

 log.Printf("Successfully processed order %s and stored receipt in S3 bucket %s",
 order.OrderID, bucketName)
 return nil
}

func main() {
 lambda.Start(handleRequest)
}
```

Ce fichier `main.go` comprend les sections suivantes :

- `package main` : dans Go, le package contenant votre fonction `func main()` doit toujours être nommé `main`.
- Bloc `import` : utilisez ce bloc pour inclure les bibliothèques que votre fonction Lambda requiert.
- Bloc `type Order struct {}` : définissez la forme de l'événement d'entrée attendu dans cette structure Go.
- Bloc `var ()` : utilisez ce bloc pour définir les variables globales que vous utiliserez dans votre fonction Lambda.
- `func init() {}` : incluez tout code que vous voulez que Lambda exécute pendant la phase d'initialisation dans cette méthode `init()`.
- `func uploadReceiptToS3(...) {}` : il s'agit d'une méthode auxiliaire référencée par la méthode de gestion principale `handleRequest`.
- `func handleRequest(ctx context.Context, event json.RawMessage) error {}` : il s'agit de la méthode de gestion principale, qui contient la logique principale de votre application.
- `func main() {}` : il s'agit d'un point d'entrée obligatoire pour votre gestionnaire Lambda. L'argument de la méthode `lambda.Start()` est votre méthode de gestion principale.

Pour que cette fonction fonctionne correctement, son rôle d'exécution doit autoriser l'action `s3:PutObject`. Assurez-vous également de définir la variable d'environnement `RECEIPT_BUCKET`. Après une invocation réussie, le compartiment Amazon S3 doit contenir un fichier de reçu.

Convention de nommage du gestionnaire

Pour les fonctions Lambda dans Go, vous pouvez utiliser n'importe quel nom pour le gestionnaire. Dans cet exemple, le nom de la méthode de traitement est `handleRequest`. Pour référencer la valeur du gestionnaire dans votre code, vous pouvez utiliser la variable d'environnement `_HANDLER`.

Pour les fonctions Go qui utilisent l'exécution dans un package de déploiement .zip, le fichier exécutable qui contient le code de votre fonction doit être nommé `bootstrap`. De plus, le fichier `bootstrap` doit se trouver à la racine du fichier .zip. Pour les fonctions Go déployées à l'aide d'une image de conteneur, vous pouvez utiliser n'importe quel nom pour le fichier exécutable.

Définition et accès à l'objet d'événement d'entrée

JSON est le format d'entrée le plus courant et standard pour les fonctions Lambda. Dans cet exemple, la fonction exige une entrée similaire à l'exemple suivant :

```
{
    "order_id": "12345",
    "amount": 199.99,
    "item": "Wireless Headphones"
}
```

Lorsque vous utilisez des fonctions Lambda dans Go, vous pouvez définir la forme de l'événement d'entrée attendu sous la forme d'une structure Go. Dans cet exemple, nous définissons une structure pour représenter un `Order` :

```
type Order struct {
    OrderID string  `json:"order_id"`
    Amount  float64 `json:"amount"`
    Item    string  `json:"item"`
}
```

Cette structure correspond à la forme d'entrée attendue. Après avoir défini votre structure, vous pouvez écrire une signature de gestionnaire qui utilise un type JSON générique compatible avec la bibliothèque encoding/json standard. Vous pouvez ensuite le désérialiser dans votre structure à l'aide de la fonction func Unmarshal. Ceci est illustré dans les premières lignes du gestionnaire :

```
func handleRequest(ctx context.Context, event json.RawMessage) error {
    // Parse the input event
    var order Order
    if err := json.Unmarshal(event, &order); err != nil {
        log.Printf("Failed to unmarshal event: %v", err)
        return err
    ...
}
```

Après cette désérialisation, vous pouvez accéder aux champs de la variable `order`. Par exemple, `order.OrderID` récupère la valeur de `"order_id"` à partir de l'entrée d'origine.

> **Note**
>
> Le package `encoding/json` ne peut accéder qu'aux champs exportés. Pour être exportées, les noms de champs de la structure d'événement doivent être en majuscules.

Accès et utilisation de l'objet de contexte Lambda

L'objet de contexte Lambda contient des informations sur l'invocation, la fonction et l'environnement d'exécution. Dans cet exemple, nous avons déclaré cette variable comme `ctx` dans la signature du gestionnaire :

```
func handleRequest(ctx context.Context, event json.RawMessage) error {
    ...
}
```

L'entrée `ctx context.Context` est un argument facultatif dans votre gestionnaire de fonctions. Pour plus d'informations sur les signatures de gestionnaire acceptées, consultez the section called "Signatures de gestionnaire valides pour les gestionnaires Go".

Si vous appelez d'autres services à l'aide du AWS SDK, l'objet de contexte est requis dans quelques domaines clés. Par exemple, pour initialiser correctement vos clients SDK, vous pouvez charger la configuration du kit SDK AWS appropriée à l'aide de l'objet de contexte comme suit :

```
// Load AWS SDK configuration using the default credential provider chain
    cfg, err := config.LoadDefaultConfig(ctx)
```

Les appels du SDK eux-mêmes peuvent nécessiter l'objet de contexte comme entrée. Par exemple, l'appel `s3Client.PutObject` accepte l'objet de contexte comme premier argument :

```
// Upload the receipt to S3
    _, err = s3Client.PutObject(ctx, &s3.PutObjectInput{
        ...
    })
```

En dehors des demandes du AWS SDK, vous pouvez également utiliser l'objet de contexte pour surveiller les fonctions. Pour plus d'informations sur la copie d'objets, consultez the section called "Contexte".

Signatures de gestionnaire valides pour les gestionnaires Go

Vous disposez de plusieurs options lorsque vous créez un gestionnaire de fonction Lambda dans Go, mais vous devez respecter les règles suivantes :

- Le gestionnaire doit être une fonction.
- Le gestionnaire peut prendre entre 0 et 2 arguments. S'il y a deux arguments, le premier argument doit implémenter `context.Context`.
- Le gestionnaire peut renvoyer entre 0 et 2 arguments. S'il y a une seule valeur renvoyée, elle doit implémenter `error`. S'il y a deux valeurs renvoyées, la seconde valeur doit implémenter `error`.

La liste suivante répertorie les signatures de gestionnaires valides. `TInet TOut` représentent des types compatibles avec la bibliothèque encoding/jsonstandard. Pour en savoir plus, reportez-vous à la section func Unmarshal pour savoir comment ces types sont désérialisés.

- `func ()`
- `func () error`
- `func () (TOut, error)`
- `func (TIn) error`
- `func (TIn) (TOut, error)`
- `func (context.Context) error`

- `func (context.Context) (TOut, error)`
- `func (context.Context, TIn) error`
- `func (context.Context, TIn) (TOut, error)`

Utilisation de AWS SDK pour Go v2 dans votre gestionnaire

Vous utiliserez souvent les fonctions Lambda pour interagir avec d'autres AWS ressources ou pour les mettre à jour. Le moyen le plus simple d'interagir avec ces ressources est d'utiliser l'AWS SDK pour Go v2.

> **Note**
>
> Le AWS SDK pour Go (v1) est en mode maintenance et atteindra la fin du support le 31 juillet 2025. Nous vous recommandons de n'utiliser que la AWS SDK pour Go v2 à l'avenir.

Pour ajouter des dépendances au SDK à votre fonction, utilisez la commande `go get` correspondant aux clients SDK spécifiques dont vous avez besoin. Dans l'exemple de code précédent, nous avons utilisé les bibliothèques `config` et `s3`. Ajoutez ces dépendances en exécutant les commandes suivantes dans le répertoire qui contient vos fichiers `go.mod` et `main.go` :

```
go get github.com/aws/aws-sdk-go-v2/config
go get github.com/aws/aws-sdk-go-v2/service/s3
```

Importez ensuite les dépendances en conséquence dans le bloc d'importation de votre fonction :

```
import (
    ...
    "github.com/aws/aws-sdk-go-v2/config"
    "github.com/aws/aws-sdk-go-v2/service/s3"
)
```

Lorsque vous utilisez le kit SDK dans votre gestionnaire, configurez vos clients avec les bons paramètres. La méthode la plus simple consiste à utiliser la chaîne de fournisseurs d'informations d'identification par défaut. Cet exemple illustre une manière de charger cette configuration :

```
// Load AWS SDK configuration using the default credential provider chain
    cfg, err := config.LoadDefaultConfig(ctx)
    if err != nil {
        log.Printf("Failed to load AWS SDK config: %v", err)
        return err
    }
```

Après avoir chargé cette configuration dans la variable `cfg`, vous pouvez transmettre cette variable aux instanciations du client. L'exemple de code crée un client Amazon S3 comme suit :

```
// Create an S3 client
    s3Client := s3.NewFromConfig(cfg)
```

Dans cet exemple, nous avons initialisé notre client Amazon S3 dans la fonction `init()` pour éviter d'avoir à l'initialiser à chaque fois que nous invoquons notre fonction. Le problème est que dans la fonction `init()`, Lambda n'a pas accès à l'objet de contexte. Pour contourner le problème, vous pouvez transmettre un espace réservé, comme `context.TODO()`, lors de la phase d'initialisation. Plus tard, lorsque vous passez un appel à l'aide du client, transmettez l'objet de contexte complet. Cette solution est également décrite dans the section called "Utilisation du contexte dans AWS Initialisations et appels du client SDK".

Après avoir configuré et initialisé votre client SDK, vous pouvez l'utiliser pour interagir avec d'autres services AWS . L'exemple de code appelle l'API Amazon S3 `PutObject` comme suit :

```
_, err = s3Client.PutObject(ctx, &s3.PutObjectInput{
    Bucket: &bucketName,
    Key:    &key,
    Body:   strings.NewReader(receiptContent),
})
```

Accès aux variables d'environnement

Dans le code de votre gestionnaire, vous pouvez référencer n'importe quelle variable d'environnement à l'aide de la méthode `os.Getenv()`. Dans cet exemple, nous référençons la variable d'environnement `RECEIPT_BUCKET` définie à l'aide de la ligne de code suivante :

```
// Access environment variables
    bucketName := os.Getenv("RECEIPT_BUCKET")
    if bucketName == "" {
        log.Printf("RECEIPT_BUCKET environment variable is not set")
```

```
        return fmt.Errorf("missing required environment variable RECEIPT_BUCKET")
    }
```

Utilisation de l'état global

Pour éviter de créer des ressources à chaque fois que vous invoquez votre fonction, vous pouvez déclarer et modifier les variables globales en dehors du code de votre gestionnaire de fonction Lambda. Vous définissez ces variables globales dans un bloc ou une instruction `var`. En outre, votre gestionnaire peut déclarer une `init()` fonction exécutée pendant la phase d'initialisation. La `init` méthode se comporte de la même manière AWS Lambda que dans les programmes Go standard.

Meilleures pratiques en matière de code pour les fonctions d'événement Go Lambda

Respectez les directives de la liste suivante pour utiliser les pratiques exemplaires de codage lors de la création de vos fonctions Lambda :

- Séparez le gestionnaire Lambda de votre logique principale. Avec cette approche, vous pouvez créer une fonction plus testable à l'unité.
- Réduisez la complexité de vos dépendances. Privilégiez les infrastructures plus simples qui se chargent rapidement au démarrage de l'environnement d'exécution.
- Réduisez la taille de votre package de déploiement selon ses besoins relatifs à l'environnement d'exécution. Cela réduit le temps nécessaire au téléchargement et au déballage de votre package de déploiement avant l'invocation.

Tirez parti de la réutilisation de l'environnement d'exécution pour améliorer les performances de votre fonction. Initialisez les clients SDK et les connexions à la base de données en dehors du gestionnaire de fonctions et mettez en cache les actifs statiques localement dans le répertoire `/tmp`. Les invocations ultérieures traitées par la même instance de votre fonction peuvent réutiliser ces ressources. Cela permet d'économiser des coûts, tout en réduisant le temps d'exécution de la fonction.

Pour éviter des éventuelles fuites de données entre les invocations, n'utilisez pas l'environnement d'exécution pour stocker des données utilisateur, des événements ou d'autres informations ayant un impact sur la sécurité. Si votre fonction repose sur un état réversible qui ne peut pas être stocké en mémoire dans le gestionnaire, envisagez de créer une fonction distincte ou des versions distinctes d'une fonction pour chaque utilisateur.

Utilisez une directive keep-alive pour maintenir les connexions persistantes. Lambda purge les connexions inactives au fil du temps. Si vous tentez de réutiliser une connexion inactive lorsque

vous invoquez une fonction, cela entraîne une erreur de connexion. Pour maintenir votre connexion persistante, utilisez la directive Keep-alive associée à votre environnement d'exécution. Pour un exemple, voir Réutilisation des connexions avec Keep-Alive in Node.js.

Utilisez des variables d'environnement pour transmettre des paramètres opérationnels à votre fonction. Par exemple, si vous écrivez dans un compartiment Amazon S3 au lieu de coder en dur le nom du compartiment dans lequel vous écrivez, configurez le nom du compartiment comme variable d'environnement.

Évitez d'utiliser des invocations récursives dans votre fonction Lambda, lorsque la fonction s'invoque elle-même ou démarre un processus susceptible de l'invoquer à nouveau. Cela peut entraîner un volume involontaire d'invocations de fonction et des coûts accrus. Si vous constatez un volume involontaire d'invocations, définissez immédiatement la simultanéité réservée à la fonction sur `0` afin de limiter toutes les invocations de la fonction, pendant que vous mettez à jour le code.

N'utilisez pas d'API non publiques non documentées dans le code de votre fonction Lambda. Pour les AWS Lambda environnements d'exécution gérés, Lambda applique régulièrement des mises à jour fonctionnelles et de sécurité aux API internes de Lambda. Ces mises à jour internes de l'API peuvent être incompatibles avec les versions antérieures, entraînant des conséquences imprévues telles que des échecs d'invocation si votre fonction dépend de ces API non publiques. Consultez la Référence d'API pour obtenir la liste des API accessibles au public.

Écriture du code idempotent. L'écriture de code idempotent pour vos fonctions garantit ne gestion identique des événements dupliqués. Votre code doit valider correctement les événements et gérer correctement les événements dupliqués. Pour de plus amples informations, veuillez consulterComment faire en sorte que ma fonction Lambda soit idempotente ?.

Utilisation de l'objet de contexte Lambda pour récupérer les informations de la fonction Go Event

Dans Lambda, l'objet de contexte fournit aux méthodes et aux propriétés des informations sur l'invocation, la fonction et l'environnement d'exécution. Lorsque Lambda exécute votre fonction, il transmet un objet contexte au gestionnaire. Pour utiliser l'objet de contexte dans votre gestionnaire, vous pouvez éventuellement le déclarer comme paramètre d'entrée dans votre gestionnaire. L'objet de contexte est nécessaire si vous souhaitez effectuer les opérations suivantes dans votre gestionnaire :

- Vous devez accéder à toutes les variables, méthodes ou propriétés globales proposées par l'objet de contexte. Ces méthodes et propriétés sont utiles pour des tâches telles que la détermination de l'entité qui a appelé votre fonction ou la mesure du temps d'invocation de votre fonction, comme illustré dans the section called "Accès aux informations du contexte d'appel".
- Vous devez utiliser le AWS SDK pour Go pour passer des appels vers d'autres services. L'objet de contexte est un paramètre d'entrée important pour la plupart de ces appels. Pour plus d'informations, consultez the section called "Utilisation du contexte dans AWS Initialisations et appels du client SDK".

Rubriques

- Variables, méthodes et propriétés prises en charge par l'objet de contexte
- Accès aux informations du contexte d'appel
- Utilisation du contexte dans AWS Initialisations et appels du client SDK

Variables, méthodes et propriétés prises en charge par l'objet de contexte

La bibliothèque de contexte Lambda fournit les variables globales, méthodes et propriétés suivantes.

Variables globales

- `FunctionName` – Nom de la fonction Lambda.
- `FunctionVersion` – Version de la fonction.
- `MemoryLimitInMB` – Quantité de mémoire allouée à la fonction.
- `LogGroupName` – Groupe de journaux pour la fonction.
- `LogStreamName` – Flux de journal de l'instance de fonction.

Méthodes de contexte

- `Deadline` – Retourne la date d'expiration de l'exécution, exprimée en millisecondes au format horaire Unix.

Propriétés du contexte

- `InvokedFunctionArn` – Amazon Resource Name (ARN) utilisé pour appeler la fonction. Indique si l'appelant a spécifié un numéro de version ou un alias.
- `AwsRequestID` – Identifiant de la demande d'appel.
- `Identity` – (applications mobiles) Informations sur l'identité Amazon Cognito qui a autorisé la demande.
- `ClientContext` – (applications mobiles) Contexte client fourni à Lambda par l'application client.

Accès aux informations du contexte d'appel

Les fonctions Lambda ont accès aux métadonnées sur leur environnement et la demande d'appel. Elles sont accessibles à l'adresse du contexte du package. Si votre gestionnaire inclut `context.Context` en tant que paramètre, Lambda insère les informations sur votre fonction dans la propriété `Value` du contexte. Notez que vous devez importer la bibliothèque `lambdacontext` pour accéder au contenu de l'objet `context.Context`.

```
package main

import (
        "context"
        "log"
        "github.com/aws/aws-lambda-go/lambda"
        "github.com/aws/aws-lambda-go/lambdacontext"
)

func CognitoHandler(ctx context.Context) {
        lc, _ := lambdacontext.FromContext(ctx)
        log.Print(lc.Identity.CognitoIdentityPoolID)
}

func main() {
        lambda.Start(CognitoHandler)
}
```

Dans l'exemple ci-dessus, la variable `lc` est-elle utilisée pour consommer les informations capturées par l'objet de contexte et `log.Print(lc.Identity.CognitoIdentityPoolID)` imprime ces informations, dans ce cas, le CognitoIdentityPoolID.

L'exemple suivant présente la façon d'utiliser l'objet contexte pour surveiller le temps nécessaire à l'exécution de votre fonction Lambda. Ainsi, vous pouvez analyser les attentes en matière de performances et ajuster votre code de fonction en conséquence, si nécessaire.

```
package main

import (
        "context"
        "log"
        "time"
        "github.com/aws/aws-lambda-go/lambda"
)

func LongRunningHandler(ctx context.Context) (string, error) {

        deadline, _ := ctx.Deadline()
        deadline = deadline.Add(-100 * time.Millisecond)
        timeoutChannel := time.After(time.Until(deadline))

        for {

                select {

                case <- timeoutChannel:
                        return "Finished before timing out.", nil

                default:
                        log.Print("hello!")
                        time.Sleep(50 * time.Millisecond)
                }
        }
}

func main() {
        lambda.Start(LongRunningHandler)
}
```

Utilisation du contexte dans AWS Initialisations et appels du client SDK

Si votre gestionnaire doit utiliser le AWS SDK pour Go pour appeler d'autres services, incluez l'objet de contexte en tant qu'entrée dans votre gestionnaire. Dans AWS, il est recommandé de transmettre l'objet de contexte dans la plupart des appels au AWS SDK. Par exemple, l'appel Amazon S3 `PutObject` accepte l'objet de contexte (`ctx`) comme premier argument :

```
// Upload an object to S3
    _, err = s3Client.PutObject(ctx, &s3.PutObjectInput{
        ...
    })
```

Pour initialiser correctement vos clients SDK, vous pouvez également utiliser l'objet de contexte pour charger la configuration correcte avant de transmettre cet objet de configuration au client :

```
// Load AWS SDK configuration using the default credential provider chain
    cfg, err := config.LoadDefaultConfig(ctx)
    ...
    s3Client = s3.NewFromConfig(cfg)
```

Si vous souhaitez initialiser vos clients SDK en dehors de votre gestionnaire principal (c'est-à-dire pendant la phase d'initialisation), vous pouvez transmettre un objet de contexte de remplacement :

```
func init() {
 // Initialize the S3 client outside of the handler, during the init phase
 cfg, err := config.LoadDefaultConfig(context.TODO())
 ...
 s3Client = s3.NewFromConfig(cfg)
}
```

Si vous initialisez vos clients de cette façon, assurez-vous de transmettre le bon objet de contexte dans les appels du SDK depuis votre gestionnaire principal.

Déployez les fonctions d'événement Go Lambda avec des archives de fichiers .zip

Le code de votre AWS Lambda fonction se compose de scripts ou de programmes compilés et de leurs dépendances. Pour déployer votre code de fonction vers Lambda, vous utilisez un package de déploiement. Lambda prend en charge deux types de packages de déploiement : les images conteneurs et les archives de fichiers .zip.

Cette page explique comment créer un fichier .zip en tant que package de déploiement pour le moteur d'exécution Go, puis utiliser le fichier .zip pour déployer votre code de fonction à AWS Lambda l'aide des Console de gestion AWS, AWS Command Line Interface (AWS CLI) et AWS Serverless Application Model (AWS SAM).

Notez que Lambda utilise des autorisations de fichier POSIX. Vous devrez donc peut-être définir des autorisations pour le dossier du package de déploiement avant de créer l'archive de fichiers .zip.

Sections

- Création d’un fichier .zip sur macOS et Linux
- Création d’un fichier .zip sous Windows
- Création et mise à jour des fonctions d'événement Go Lambda à l'aide de fichiers .zip

Création d’un fichier .zip sur macOS et Linux

Les étapes suivantes montrent comment compiler votre exécutable à l’aide de la commande go `build` et créer un package de déploiement de fichiers .zip pour Lambda. Avant de compiler votre code, assurez-vous d'avoir installé le package lambda depuis. GitHub Ce module fournit une implémentation de l’interface d’exécution, qui gère l’interaction entre Lambda et le code de votre fonction. Pour télécharger cette bibliothèque, exécutez la commande suivante.

```
go get github.com/aws/aws-lambda-go/lambda
```

Si votre fonction utilise le AWS SDK pour Go, téléchargez l'ensemble standard de modules du SDK, ainsi que tous les clients d'API de AWS service requis par votre application. Pour savoir comment installer le SDK pour Go, consultez Getting Started with AWS SDK pour Go the V2.

Utilisation de la famille d’environnement d’exécution fournie

Go est implémenté différemment des autres exécutions gérées. Go se compilant nativement en un binaire exécutable, il n’a pas besoin d’un environnement d’exécution dédié au langage. Utilisez

un OS-only environnement d'exécution (la famille `provided` d'exécution) pour déployer Go Event Functions sur Lambda.

Pour créer un package de déploiement .zip () macOS/Linux

1. Dans le répertoire du projet qui contient le fichier `main.go` de votre application, compilez votre exécutable. Notez ce qui suit :

   - L'exécutable doit être nommé `bootstrap`. Pour plus d'informations, consultez Convention de nommage du gestionnaire.
   - Définissez l'architecture de votre jeu d'instructions cible. OS-only les environnements d'exécution supportent à la fois arm64 et x86_64.
   - Vous pouvez utiliser la balise optionnelle `lambda.norpc` pour exclure le composant RPC (Remote Procedure Call) de la bibliothèque lambda. Le composant RPC n'est nécessaire que lorsque vous utilisez l'environnement d'exécution Go 1.x. L'exclusion du RPC réduit la taille du package de déploiement.

   Pour l'architecture arm64 :

   ```
   GOOS=linux GOARCH=arm64 go build -tags lambda.norpc -o bootstrap main.go
   ```

   Pour l'architecture x86_64 :

   ```
   GOOS=linux GOARCH=amd64 go build -tags lambda.norpc -o bootstrap main.go
   ```

2. (Facultatif) Vous devrez peut-être compiler des packages avec `CGO_ENABLED=0` configuré sur Linux :

   ```
   GOOS=linux GOARCH=arm64 CGO_ENABLED=0 go build -o bootstrap -tags lambda.norpc
    main.go
   ```

   Cette commande crée un package binaire stable pour les versions de bibliothèque C standard (`libc`), qui peuvent être différentes sur Lambda et d'autres appareils.

3. Créez un package de déploiement en empaquetant l'exécutable dans un fichier .zip.

   ```
   zip myFunction.zip bootstrap
   ```

> **Note**
>
> Le fichier `bootstrap` doit se situer à la racine du fichier .zip.

4. Créez la fonction . Notez ce qui suit :

   - Le binaire doit être nommé `bootstrap`, mais le nom du gestionnaire peut être quelconque. Pour plus d'informations, consultez Convention de nommage du gestionnaire.
   - L'option `--architectures` n'est nécessaire que si vous utilisez arm64. La valeur par défaut est x86_64.
   - Pour `--role`, spécifiez l'Amazon Resource Name (ARN) du rôle d'exécution.

```
aws lambda create-function --function-name myFunction \
--runtime provided.al2023 --handler bootstrap \
--architectures arm64 \
--role arn:aws:iam::111122223333:role/lambda-ex \
--zip-file fileb://myFunction.zip
```

Création d'un fichier .zip sous Windows

Les étapes suivantes indiquent comment télécharger l'outil build-lambda-zip pour Windows depuis GitHub, compiler votre exécutable et créer un package de déploiement .zip.

> **Note**
>
> Si vous ne l'avez pas déjà fait, vous devez installer git, puis ajouter l'exécutable `git` à votre variable d'environnement Windows `%PATH%`.

Avant de compiler votre code, assurez-vous d'avoir installé la bibliothèque Lambda depuis. GitHub Pour télécharger cette bibliothèque, exécutez la commande suivante.

```
go get github.com/aws/aws-lambda-go/lambda
```

Si votre fonction utilise le AWS SDK pour Go, téléchargez l'ensemble standard de modules du SDK, ainsi que tous les clients d'API de AWS service requis par votre application. Pour savoir comment installer le SDK pour Go, consultez Getting Started with AWS SDK pour Go the V2.

Utilisation de la famille d'environnement d'exécution fournie

Go est implémenté différemment des autres exécutions gérées. Go se compilant nativement en un binaire exécutable, il n'a pas besoin d'un environnement d'exécution dédié au langage. Utilisez un OS-only environnement d'exécution (la famille `provided` d'exécution) pour déployer Go Event Functions sur Lambda.

Pour créer un package de déploiement .zip (Windows)

1. Téléchargez l'outil build-lambda-zip depuis. GitHub

   ```
   go install github.com/aws/aws-lambda-go/cmd/build-lambda-zip@latest
   ```

2. Utilisez l'outil de votre `GOPATH` pour créer un fichier .zip. Si vous disposez d'une installation de Go par défaut, l'outil est généralement dans `%USERPROFILE%\Go\bin`. Dans le cas contraire, accédez à l'endroit où vous avez installé l'environnement d'exécution Go et effectuez l'une des instructions suivantes :

   cmd.exe

   Dans le fichier cmd.exe, exécutez l'une des opérations suivantes, en fonction de l'architecture de votre jeu d'instructions cible. OS-only les environnements d'exécution supportent à la fois arm64 et x86_64.

   Vous pouvez utiliser la balise optionnelle `lambda.norpc` pour exclure le composant RPC (Remote Procedure Call) de la bibliothèque lambda. Le composant RPC n'est nécessaire que lorsque vous utilisez l'environnement d'exécution Go 1.x. L'exclusion du RPC réduit la taille du package de déploiement.

   Example— Pour l'architecture x86_64

   ```
   set GOOS=linux
   set GOARCH=amd64
   set CGO_ENABLED=0
   go build -tags lambda.norpc -o bootstrap main.go
   %USERPROFILE%\Go\bin\build-lambda-zip.exe -o myFunction.zip bootstrap
   ```

Example— Pour l'architecture arm64

```
set GOOS=linux
set GOARCH=arm64
set CGO_ENABLED=0
go build -tags lambda.norpc -o bootstrap main.go
%USERPROFILE%\Go\bin\build-lambda-zip.exe -o myFunction.zip bootstrap
```

PowerShell

Dans PowerShell, exécutez l'une des opérations suivantes, en fonction de l'architecture de votre jeu d'instructions cible. OS-only les environnements d'exécution supportent à la fois arm64 et x86_64.

Vous pouvez utiliser la balise optionnelle `lambda.norpc` pour exclure le composant RPC (Remote Procedure Call) de la bibliothèque lambda. Le composant RPC n'est nécessaire que lorsque vous utilisez l'environnement d'exécution Go 1.x. L'exclusion du RPC réduit la taille du package de déploiement.

Pour l'architecture x86_64 :

```
$env:GOOS = "linux"
$env:GOARCH = "amd64"
$env:CGO_ENABLED = "0"
go build -tags lambda.norpc -o bootstrap main.go
~\Go\Bin\build-lambda-zip.exe -o myFunction.zip bootstrap
```

Pour l'architecture arm64 :

```
$env:GOOS = "linux"
$env:GOARCH = "arm64"
$env:CGO_ENABLED = "0"
go build -tags lambda.norpc -o bootstrap main.go
~\Go\Bin\build-lambda-zip.exe -o myFunction.zip bootstrap
```

3. Créez la fonction . Notez ce qui suit :

- Le binaire doit être nommé `bootstrap`, mais le nom du gestionnaire peut être quelconque. Pour plus d'informations, consultez Convention de nommage du gestionnaire.

- L'option `--architectures` n'est nécessaire que si vous utilisez arm64. La valeur par défaut est x86_64.
- Pour `--role`, spécifiez l'Amazon Resource Name (ARN) du rôle d'exécution.

```
aws lambda create-function --function-name myFunction \
--runtime provided.al2023 --handler bootstrap \
--architectures arm64 \
--role arn:aws:iam::111122223333:role/lambda-ex \
--zip-file fileb://myFunction.zip
```

Création et mise à jour des fonctions d'événement Go Lambda à l'aide de fichiers .zip

Une fois que vous avez créé votre package de déploiement .zip, vous pouvez l'utiliser pour créer une nouvelle fonction Lambda ou mettre à jour une fonction Lambda existante. Vous pouvez déployer votre package .zip à l'aide de la console Lambda, de l'API Lambda et AWS Command Line Interface de l'API Lambda. Vous pouvez également créer et mettre à jour des fonctions Lambda à l'aide de l' AWS Serverless Application Model (AWS SAM) et de CloudFormation.

La taille maximale d'un package de déploiement .zip pour Lambda est de 250 Mo (décompressé). Notez que cette limite s'applique à la taille combinée de tous les fichiers que vous chargez, y compris les couches Lambda.

Le runtime Lambda a besoin d'une autorisation pour lire les fichiers de votre package de déploiement. Dans la notation octale des autorisations Linux, Lambda a besoin de 644 autorisations pour les fichiers non exécutables (rw-r--r--) et de 755 autorisations (rwxr-xr-x) pour les répertoires et les fichiers exécutables.

Sous Linux et macOS, utilisez la commande chmod pour modifier les autorisations de fichiers sur les fichiers et les répertoires de votre package de déploiement. Par exemple, pour octroyer à un fichier non exécutable les autorisations correctes, exécutez la commande suivante.

```
chmod 644 <filepath>
```

Pour modifier les autorisations relatives aux fichiers dans Windows, voir Définir, afficher, modifier ou supprimer des autorisations sur un objet dans la documentation Microsoft Windows.

> **Note**
>
> Si vous n'octroyez pas à Lambda les autorisations dont il a besoin pour accéder aux répertoires de votre package de déploiement, Lambda définit les autorisations de ces répertoires à 755 (rwxr-xr-x).

Création et mise à jour de fonctions avec des fichiers .zip à l'aide de la console

Pour créer une nouvelle fonction, vous devez d'abord créer la fonction dans la console, puis charger votre archive .zip. Pour mettre à jour une fonction existante, ouvrez la page de votre fonction, puis suivez la même procédure pour ajouter votre fichier .zip mis à jour.

Si votre fichier .zip fait moins de 50 Mo, vous pouvez créer ou mettre à jour une fonction en chargeant le fichier directement à partir de votre ordinateur local. Pour les fichiers .zip de plus de 50 Mo, vous devez d'abord charger votre package dans un compartiment Amazon S3. Pour savoir comment charger un fichier dans un compartiment Amazon S3 à l'aide du Console de gestion AWS, consultez Getting started with Amazon S3. Pour télécharger des fichiers à l'aide de AWS CLI, voir Déplacer des objets dans le guide de AWS CLI l'utilisateur.

> **Note**
>
> Vous ne pouvez pas convertir une fonction d'image de conteneur existante pour utiliser une archive .zip. Vous devez créer une nouvelle fonction.

Pour créer une nouvelle fonction (console)

1. Ouvrez la page Event Functions de la console Lambda et choisissez Create Event Function.
2. Choisissez Créer à partir de zéro.
3. Sous Informations de base, procédez comme suit :
   a. Pour Nom de la fonction, saisissez le nom de la fonction.
   b. Dans Runtime (Exécution), choisissez `provided.al2023`.
4. (Facultatif) Sous Permissions (Autorisations), développez Change default execution role (Modifier le rôle d'exécution par défaut). Vous pouvez créer un rôle d'exécution ou en utiliser un existant.

5. Choisissez Create Event Function. Lambda crée une fonction de base « Hello world » à l'aide de l'exécution de votre choix.

Pour charger une archive .zip à partir de votre ordinateur local (console)

1. Sur la page Event Functions de la console Lambda, choisissez la fonction pour laquelle vous souhaitez télécharger le fichier .zip.
2. Sélectionnez l'onglet Code.
3. Dans le volet Source du code, choisissez Charger à partir de.
4. Choisissez Fichier .zip.
5. Pour charger un fichier .zip, procédez comme suit :
   a. Sélectionnez Charger, puis choisissez votre fichier .zip dans le sélecteur de fichiers.
   b. Choisissez Ouvrir.
   c. Cliquez sur Enregistrer.

Pour charger une archive .zip depuis un compartiment Amazon S3 (console)

1. Sur la page Event Functions de la console Lambda, choisissez la fonction pour laquelle vous souhaitez télécharger un nouveau fichier .zip.
2. Sélectionnez l'onglet Code.
3. Dans le volet Source du code, choisissez Charger à partir de.
4. Choisissez l'emplacement Amazon S3.
5. Collez l'URL du lien Amazon S3 de votre fichier .zip et choisissez Enregistrer.

Création et mise à jour de fonctions avec des fichiers .zip à l'aide du AWS CLI

Vous pouvez utiliser l'AWS CLI pour créer une nouvelle fonction ou pour mettre à jour une fonction existante à l'aide d'un fichier .zip. Utilisez les commandes create-function et update-function-code pour déployer votre package .zip. Si votre fichier .zip est inférieur à 50 Mo, vous pouvez charger le package .zip à partir d'un emplacement de fichier sur votre machine de génération locale. Pour les fichiers plus volumineux, vous devez charger votre package .zip à partir d'un compartiment Amazon S3. Pour savoir comment charger un fichier dans un compartiment Amazon S3 à l'aide du AWS CLI, consultez la section Déplacer des objets dans le guide de AWS CLI l'utilisateur.

> **Note**
>
> Si vous chargez votre fichier .zip depuis un compartiment Amazon S3 à l'aide de AWS CLI, le compartiment doit se trouver au même endroit Région AWS que votre fonction.

Pour créer une nouvelle fonction à l'aide d'un fichier .zip avec le AWS CLI, vous devez spécifier les éléments suivants :

- Le nom de votre fonction (`--function-name`)
- L'exécution de votre fonction (`--runtime`)
- L'Amazon Resource Name (ARN) du rôle d'exécution de votre fonction (`--role`)
- Le nom de la méthode du gestionnaire dans votre code de fonction (`--handler`)

Vous devez également indiquer l'emplacement de votre fichier .zip. Si votre fichier .zip se trouve dans un dossier sur votre machine de génération locale, utilisez l'option `--zip-file` pour spécifier le chemin d'accès du fichier, comme le montre l'exemple de commande suivant.

```
aws lambda create-function --function-name myFunction \
--runtime provided.al2023 --handler bootstrap \
--role arn:aws:iam::111122223333:role/service-role/my-lambda-role \
--zip-file fileb://myFunction.zip
```

Pour spécifier l'emplacement du fichier .zip dans un compartiment Amazon S3, utilisez l'option `--code` comme le montre l'exemple de commande suivant. Vous devez uniquement utiliser le paramètre `S3ObjectVersion` pour les objets soumis à la gestion des versions.

```
aws lambda create-function --function-name myFunction \
--runtime provided.al2023 --handler bootstrap \
--role arn:aws:iam::111122223333:role/service-role/my-lambda-role \
--code S3Bucket=amzn-s3-demo-
bucket,S3Key=myFileName.zip,S3ObjectVersion=myObjectVersion
```

Pour mettre à jour une fonction existante à l'aide de l'interface de ligne de commande, vous devez spécifier le nom de votre fonction à l'aide du paramètre `--function-name`. Vous devez également spécifier l'emplacement du fichier .zip que vous souhaitez utiliser pour mettre à jour votre code de fonction. Si votre fichier .zip se trouve dans un dossier sur votre machine de génération locale,

utilisez l'option `--zip-file` pour spécifier le chemin d'accès du fichier, comme le montre l'exemple de commande suivant.

```
aws lambda update-function-code --function-name myFunction \
--zip-file fileb://myFunction.zip
```

Pour spécifier l'emplacement du fichier .zip dans un compartiment Amazon S3, utilisez les options `--s3-bucket` et `--s3-key` comme le montre l'exemple de commande suivant. Vous devez uniquement utiliser le paramètre `--s3-object-version` pour les objets soumis à la gestion des versions.

```
aws lambda update-function-code --function-name myFunction \
--s3-bucket amzn-s3-demo-bucket --s3-key myFileName.zip --s3-object-version myObject
 Version
```

Création et mise à jour de fonctions avec des fichiers .zip à l'aide de l'API Lambda

Pour créer et mettre à jour des fonctions à l'aide d'une archive de fichiers .zip, utilisez les opérations d'API suivantes :

- CreateFunction
- UpdateFunctionCode

Création et mise à jour de fonctions avec des fichiers .zip à l'aide de AWS SAM

The AWS Serverless Application Model (AWS SAM) est une boîte à outils qui permet de rationaliser le processus de création et d'exécution d'applications sans serveur sur AWS. Vous définissez les ressources de votre application dans un modèle YAML ou JSON et vous utilisez l'interface de ligne de AWS SAM commande (AWS SAM CLI) pour créer, empaqueter et déployer vos applications. Lorsque vous créez une fonction Lambda à partir d'un AWS SAM modèle, elle crée AWS SAM automatiquement un package de déploiement ou une image de conteneur .zip avec le code de votre fonction et les dépendances que vous spécifiez. Pour en savoir plus sur l'utilisation des fonctions Lambda AWS SAM pour créer et déployer des fonctions Lambda, consultez la section Getting started with AWS SAM dans le Guide du AWS Serverless Application Model développeur.

Vous pouvez également l'utiliser AWS SAM pour créer une fonction Lambda à l'aide d'une archive de fichiers .zip existante. Pour créer une fonction Lambda à l'aide de AWS SAM, vous pouvez enregistrer votre fichier .zip dans un compartiment Amazon S3 ou dans un dossier local sur votre

machine de génération. Pour savoir comment charger un fichier dans un compartiment Amazon S3 à l'aide du AWS CLI, consultez la section Déplacer des objets dans le guide de AWS CLI l'utilisateur.

Dans votre AWS SAM modèle, la `AWS::Serverless::Function` ressource spécifie votre fonction Lambda. Dans cette ressource, définissez les propriétés suivantes pour créer une fonction à l'aide d'une archive de fichiers .zip :

- `PackageType` : défini sur `Zip`
- `CodeUri`- défini sur l'URI Amazon S3, le chemin d'accès au dossier local ou à l'FunctionCodeobjet du code de fonction
- `Runtime` : défini sur votre exécution choisie

Ainsi AWS SAM, si votre fichier .zip est supérieur à 50 Mo, vous n'avez pas besoin de le télécharger au préalable dans un compartiment Amazon S3. AWS SAM peut télécharger des packages .zip jusqu'à la taille maximale autorisée de 250 Mo (décompressés) à partir d'un emplacement sur votre machine de compilation locale.

Pour en savoir plus sur le déploiement de fonctions à l'aide d'un fichier .zip dans AWS SAM, voir AWS::Serverless::Function dans le manuel du AWS SAM développeur.

Exemple : utilisation AWS SAM pour créer une fonction Go avec provided.al2023

1. Créez un AWS SAM modèle avec les propriétés suivantes :

   - BuildMethod: Spécifie le compilateur de votre application. Utilisez `go1.x`.
   - Runtime : utilisez `provided.al2023`.
   - CodeUri: Entrez le chemin d'accès à votre code.
   - Architectures : Utilisez `[arm64]` pour l'architecture arm64. Pour l'architecture x86_64, utilisez `[amd64]` ou supprimez la propriété `Architectures`.

   Example template.yaml

   ```
   AWSTemplateFormatVersion: '2010-09-09'
   Transform: 'AWS::Serverless-2016-10-31'
   Resources:
     HelloWorldFunction:
       Type: AWS::Serverless::Function
       Metadata:
         BuildMethod: go1.x
   ```

```
    Properties:
      CodeUri: hello-world/ # folder where your main program resides
      Handler: bootstrap
      Runtime: provided.al2023
      Architectures: [arm64]
```

2. Utilisez la commande sam build pour compiler l'exécutable.

```
sam build
```

3. Utilisez la commande sam deploy pour déployer la fonction vers Lambda.

```
sam deploy --guided
```

Création et mise à jour de fonctions avec des fichiers .zip à l'aide de CloudFormation

Vous pouvez l'utiliser CloudFormation pour créer une fonction Lambda à l'aide d'une archive de fichiers .zip. Pour créer une fonction Lambda à partir d'un fichier .zip, vous devez d'abord charger votre fichier dans un compartiment Amazon S3. Pour savoir comment charger un fichier dans un compartiment Amazon S3 à l'aide du AWS CLI, consultez la section Déplacer des objets dans le guide de AWS CLI l'utilisateur.

Dans votre CloudFormation modèle, la `AWS::Lambda::Function` ressource spécifie votre fonction Lambda. Dans cette ressource, définissez les propriétés suivantes pour créer une fonction à l'aide d'une archive de fichiers .zip :

- `PackageType` : défini sur `Zip`
- `Code` : saisissez le nom du compartiment Amazon S3 et le nom du fichier .zip dans les champs `S3Bucket` et `S3Key`
- `Runtime` : défini sur votre exécution choisie

Le fichier .zip CloudFormation généré ne peut pas dépasser 4 Mo. Pour en savoir plus sur le déploiement de fonctions à l'aide d'un fichier .zip dans CloudFormation, voir AWS::Lambda::Function dans le guide de l'CloudFormation utilisateur.

Déployez les fonctions d'événement Go Lambda avec des images de conteneur

Il existe deux manières de créer une image de conteneur pour une fonction d'événement Go Lambda :

- À l'aide d'un AWS OS-only image de base

  Go est implémenté différemment des autres exécutions gérées. Go se compilant nativement en un binaire exécutable, il n'a pas besoin d'un environnement d'exécution dédié au langage. Utilisez une image OS-only de base pour créer des images Go pour Lambda. Pour rendre l'image compatible avec Lambda, vous devez inclure le package `aws-lambda-go/lambda` dans l'image.

- En utilisant un non-AWS image de base

  Vous pouvez utiliser une autre image de base à partir d'un autre registre de conteneur, comme Alpine Linux ou Debian. Vous pouvez également utiliser une image personnalisée créée par votre organisation. Pour rendre l'image compatible avec Lambda, vous devez inclure le package `aws-lambda-go/lambda` dans l'image.

> **Tip**
>
> Pour réduire le temps nécessaire à l'activation des fonctions du conteneur Lambda, consultez Utiliser des générations en plusieurs étapes (français non garanti) dans la documentation Docker. Pour créer des images de conteneur efficaces, suivez la section Bonnes pratiques pour l'écriture de Dockerfiles (français non garanti).

Cette page explique comment créer, tester et déployer des images de conteneur pour Lambda.

AWS images de base pour le déploiement des fonctions Go

Go est implémenté différemment des autres exécutions gérées. Go se compilant nativement en un binaire exécutable, il n'a pas besoin d'un environnement d'exécution dédié au langage. Utilisez une image OS-only de base pour déployer les fonctions Go sur Lambda.

Nom	Identifiant	Système d'exploitation	Date d'obsolescence	Créer la fonction de blocage	Mettre à jour la fonction de blocage
OS-only Temps d'exécution	`provided.al2023`	Amazon Linux 2	30 juin 2029	31 juillet 2029	31 août 2029

Galerie publique d'Amazon Elastic Container Registry : gallery.ecr. aws/lambda/fourni

Client d'interface d'environnement d'exécution Go

Le package `aws-lambda-go/lambda` inclut une implémentation de l'interface d'exécution. Pour obtenir des exemples d'utilisation de `aws-lambda-go/lambda` dans votre image, consultez À l'aide d'un AWS OS-only image de base ou En utilisant un non-AWS image de base.

À l'aide d'un AWS OS-only image de base

Go est implémenté différemment des autres exécutions gérées. Go se compilant nativement en un binaire exécutable, il n'a pas besoin d'un environnement d'exécution dédié au langage. Utilisez une image OS-only de base pour créer des images de conteneur pour les fonctions Go.

Étiquettes	Environnement d'exécution	Système d'exploitation	Dockerfile	Obsolescence
al2023	OS-only Temps d'exécution	Amazon Linux	Dockerfile pour OS-only Runtime sur GitHub	30 juin 2029

Pour plus d'informations sur ces images de base, consultez fourni située dans la galerie publique Amazon ECR.

Vous devez inclure le go/lambda package aws-lambda- dans votre gestionnaire Go. Ce package implémente le modèle de programmation pour Go, y compris l'interface d'exécution.

Conditions préalables

Pour exécuter la procédure indiquée dans cette section, vous devez satisfaire aux exigences suivantes :

- AWS CLI version 2
- Docker (version minimale 25.0.0)
- Le plug-in buildx Docker.
- Go

Création d'une image à partir de l'image de base provided.al2023

Pour créer et déployer une fonction Go avec l'image de base **`.al2023 fournie`**

1. Créez un répertoire pour le projet, puis passez à ce répertoire.

```
mkdir hello
cd hello
```

2. Initialisez un nouveau module Go.

```
go mod init example.com/hello-world
```

3. Ajoutez la bibliothèque lambda comme dépendance de votre nouveau module.

```
go get github.com/aws/aws-lambda-go/lambda
```

4. Créez un fichier nommé `main.go` et ouvrez-le dans un éditeur de texte. Il s'agit du code de la fonction Lambda. Vous pouvez utiliser l'exemple de code suivant pour le tester, ou le remplacer par le vôtre.

```
package main

import (
 "context"
 "github.com/aws/aws-lambda-go/events"
 "github.com/aws/aws-lambda-go/lambda"
)
```

```
func handler(ctx context.Context, event events.APIGatewayProxyRequest)
 (events.APIGatewayProxyResponse, error) {
 response := events.APIGatewayProxyResponse{
  StatusCode: 200,
  Body:       "\"Hello from Lambda!\"",
 }
 return response, nil
}

func main() {
 lambda.Start(handler)
}
```

5. Utilisez un éditeur de texte afin de créer un Dockerfile dans votre répertoire de projets.

   - L'exemple suivant Dockerfile utilise une version en plusieurs étapes sur le site Web de documentation Docker. Avec une construction en plusieurs étapes, vous pouvez utiliser une image de base différente à chaque étape. Vous pouvez utiliser une image, telle qu'une image de base Go sur Docker Hub, pour compiler votre code et créer le binaire exécutable. Vous pouvez ensuite utiliser une image différente, telle que `provided.al2023`, dans l'instruction finale `FROM` pour définir l'image que vous déployez sur Lambda. La génération en plusieurs étapes sépare le processus de génération de l'image de déploiement finale, de sorte que l'image finale ne contient que les fichiers nécessaires à l'exécution de l'application.
   - Vous pouvez utiliser la balise optionnelle `lambda.norpc` pour exclure le composant RPC (Remote Procedure Call) de la bibliothèque lambda. Le composant RPC n'est nécessaire que lorsque vous utilisez l'environnement d'exécution Go 1.x. L'exclusion du RPC réduit la taille du package de déploiement.
   - Notez que l'exemple de Dockerfile n'inclut pas d'instruction USER. Lorsque vous déployez une image de conteneur sur Lambda, Lambda définit automatiquement un utilisateur Linux par défaut disposant d'autorisations de moindre privilège. Ceci est différent du comportement standard de Docker qui est défini par défaut par l'utilisateur `root` lorsqu'aucune instruction `USER` n'est fournie.

Example— Multi-stage construit Dockerfile

> **Note**
>
> Assurez-vous que la version de Go que vous spécifiez dans votre Dockerfile (par exemple, `golang:1.20`) est la même que celle que vous avez utilisée pour créer votre application.

```
FROM golang:1.20 as build
WORKDIR /helloworld
# Copy dependencies list
COPY go.mod go.sum ./
# Build with optional lambda.norpc tag
COPY main.go .
RUN go build -tags lambda.norpc -o main main.go
# Copy artifacts to a clean image
FROM public.ecr.aws/lambda/provided:al2023
COPY --from=build /helloworld/main ./main
ENTRYPOINT [ "./main" ]
```

6. Générez l'image Docker à l'aide de la commande docker build. L'exemple suivant nomme l'image `docker-image` et lui donne la balise `test`. Pour rendre votre image compatible avec Lambda, vous devez utiliser l'option `--provenance=false`.

```
docker buildx build --platform linux/amd64 --provenance=false -t docker-image:test
 .
```

> **Note**
>
> La commande spécifie l'option `--platform linux/amd64` pour garantir la compatibilité de votre conteneur avec l'environnement d'exécution Lambda, quelle que soit l'architecture de votre machine de génération. Si vous avez l'intention de créer une fonction Lambda à l'aide de l'architecture du jeu d'instructions ARM64, veillez à modifier la commande pour utiliser plutôt l'option `--platform linux/arm64`.

(Facultatif) Testez l'image localement

Utilisez l'émulateur d'interface d'exécution pour tester votre image localement. L'émulateur d'interface d'exécution est inclus dans l'image de base `provided.al2023`.

Pour exécuter l'émulateur d'interface d'exécution sur votre ordinateur local

1. Démarrez votre image Docker à l'aide de la commande docker run. Notez ce qui suit :

   - `docker-image` est le nom de l'image et `test` est la balise.
   - `./main` est le `ENTRYPOINT` de votre Dockerfile.

   ```
   docker run -d -p 9000:8080 \
   --entrypoint /usr/local/bin/aws-lambda-rie \
   docker-image:test ./main
   ```

   Cette commande exécute l'image en tant que conteneur et crée un point de terminaison local à `localhost:9000/2015-03-31/functions/function/invocations`.

2. À partir d'une nouvelle fenêtre de terminal, publiez un événement sur le point de terminaison suivant au moyen d'une commande curl :

   ```
   curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d '{}'
   ```

   Cette commande invoque la fonction avec un événement vide et renvoie une réponse. Certaines fonctions peuvent nécessiter l'ajout d'une charge utile JSON. Exemple :

   ```
   curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d
    '{"payload":"hello world!"}'
   ```

3. Obtenez l'ID du conteneur.

   ```
   docker ps
   ```

4. Utilisez la commande docker kill pour arrêter le conteneur. Dans cette commande, remplacez `3766c4ab331c` par l'ID du conteneur de l'étape précédente.

   ```
   docker kill 3766c4ab331c
   ```

Déploiement de l'image

Pour charger l'image sur Amazon RIE et créer la fonction Lambda

1. Exécutez la commande get-login-password pour authentifier la CLI Docker auprès de votre registre Amazon ECR.

   - Définissez la `--region` valeur à l' Région AWS endroit où vous souhaitez créer le référentiel Amazon ECR.
   - `111122223333`Remplacez-le par votre Compte AWS identifiant.

   ```
   aws ecr get-login-password --region us-east-1 | docker login --username AWS --
   password-stdin 111122223333.dkr.ecr.us-east-1.amazonaws.com
   ```

2. Créez un référentiel dans Amazon ECR à l'aide de la commande create-repository.

   ```
   aws ecr create-repository --repository-name hello-world --region us-east-1 --image-
   scanning-configuration scanOnPush=true --image-tag-mutability MUTABLE
   ```

   > **Note**
   >
   > Le référentiel Amazon ECR doit être Région AWS identique à la fonction Lambda.

   En cas de succès, vous obtenez une réponse comme celle-ci :

   ```
   {
       "repository": {
           "repositoryArn": "arn:aws:ecr:us-east-1:111122223333:repository/hello-
   world",
           "registryId": "111122223333",
           "repositoryName": "hello-world",
           "repositoryUri": "111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-
   world",
           "createdAt": "2023-03-09T10:39:01+00:00",
           "imageTagMutability": "MUTABLE",
           "imageScanningConfiguration": {
               "scanOnPush": true
           },
           "encryptionConfiguration": {
   ```

```
            "encryptionType": "AES256"
        }
    }
}
```

3. Copiez le `repositoryUri` à partir de la sortie de l'étape précédente.
4. Exécutez la commande docker tag pour étiqueter votre image locale dans votre référentiel Amazon ECR en tant que dernière version. Dans cette commande :
   - `docker-image:test` est le nom et la balise de votre image Docker. Il s'agit du nom et de la balise de l'image que vous avez spécifiés dans la commande `docker build`.
   - Remplacez <ECRrepositoryUri> par l'`repositoryUri` que vous avez copié. Assurez-vous d'inclure `:latest` à la fin de l'URI.

   ```
   docker tag docker-image:test <ECRrepositoryUri>:latest
   ```

   Exemple :

   ```
   docker tag docker-image:test 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
   ```
5. Exécutez la commande docker push pour déployer votre image locale dans le référentiel Amazon ECR. Assurez-vous d'inclure `:latest` à la fin de l'URI du référentiel.

   ```
   docker push 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
   ```
6. Créez un rôle d'exécution pour la fonction, si vous n'en avez pas déjà un. Vous aurez besoin de l'Amazon Resource Name (ARN) du rôle à l'étape suivante.
7. Créez la fonction Lambda. Pour `ImageUri`, indiquez l'URI du référentiel mentionné précédemment. Assurez-vous d'inclure `:latest` à la fin de l'URI.

   ```
   aws lambda create-function \
     --function-name hello-world \
     --package-type Image \
     --code ImageUri=111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \
     --role arn:aws:iam::111122223333:role/lambda-ex
   ```

> **Note**
>
> Vous pouvez créer une fonction en utilisant une image d'un autre AWS compte, à condition que l'image se trouve dans la même région que la fonction Lambda. Pour plus d'informations, consultez Autorisations entre comptes Amazon ECR.

8. Invoquer la fonction.

```
aws lambda invoke --function-name hello-world response.json
```

Vous devriez obtenir une réponse comme celle-ci :

```
{
  "ExecutedVersion": "$LATEST",
  "StatusCode": 200
}
```

9. Pour voir la sortie de la fonction, consultez le fichier `response.json`.

Pour mettre à jour le code de la fonction, vous devez recréer l'image, charger la nouvelle image dans le référentiel Amazon ECR, puis utiliser la commande update-function-code pour déployer l'image dans la fonction Lambda.

Lambda résout l'étiquette d'image en hachage d'image spécifique. Cela signifie que si vous pointez la balise d'image qui a été utilisée pour déployer la fonction vers une nouvelle image dans Amazon ECR, Lambda ne met pas automatiquement à jour la fonction pour utiliser la nouvelle image.

Pour déployer la nouvelle image sur la même fonction Lambda, vous devez utiliser la commande update-function-code, même si la balise d'image dans Amazon ECR reste la même. Dans l'exemple suivant, l'option `--publish` crée une version de la fonction à l'aide de l'image du conteneur mise à jour.

```
aws lambda update-function-code \
  --function-name hello-world \
  --image-uri 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \
  --publish
```

En utilisant un non-AWS image de base

Vous pouvez créer une image de conteneur pour Go à partir d'une image non AWS basique. L'exemple de Dockerfile dans les étapes suivantes utilise une image de base Alpine.

Vous devez inclure le go/lambda package aws-lambda- dans votre gestionnaire Go. Ce package implémente le modèle de programmation pour Go, y compris l'interface d'exécution.

Conditions préalables

Pour exécuter la procédure indiquée dans cette section, vous devez satisfaire aux exigences suivantes :

- AWS CLI version 2
- Docker (version minimale 25.0.0)
- Le plug-in buildx Docker.
- Go

Création d'une image à partir d'une image de base alternative

Pour créer et déployer une fonction Go avec une image de base Alpine

1. Créez un répertoire pour le projet, puis passez à ce répertoire.

```
mkdir hello
cd hello
```

2. Initialisez un nouveau module Go.

```
go mod init example.com/hello-world
```

3. Ajoutez la bibliothèque lambda comme dépendance de votre nouveau module.

```
go get github.com/aws/aws-lambda-go/lambda
```

4. Créez un fichier nommé `main.go` et ouvrez-le dans un éditeur de texte. Il s'agit du code de la fonction Lambda. Vous pouvez utiliser l'exemple de code suivant pour le tester, ou le remplacer par le vôtre.

```
package main
```

```
import (
 "context"
 "github.com/aws/aws-lambda-go/events"
 "github.com/aws/aws-lambda-go/lambda"
)

func handler(ctx context.Context, event events.APIGatewayProxyRequest)
 (events.APIGatewayProxyResponse, error) {
 response := events.APIGatewayProxyResponse{
  StatusCode: 200,
  Body:       "\"Hello from Lambda!\"",
 }
 return response, nil
}

func main() {
 lambda.Start(handler)
}
```

5. Utilisez un éditeur de texte afin de créer un Dockerfile dans votre répertoire de projets. L'exemple de Dockerfile suivant utilise une image de base Alpine. Notez que l'exemple de Dockerfile n'inclut pas d'instruction USER. Lorsque vous déployez une image de conteneur sur Lambda, Lambda définit automatiquement un utilisateur Linux par défaut disposant d'autorisations de moindre privilège. Ceci est différent du comportement standard de Docker qui est défini par défaut par l'utilisateur `root` lorsqu'aucune instruction USER n'est fournie.

   Example Dockerfile

   > **Note**
   >
   > Assurez-vous que la version de Go que vous spécifiez dans votre Dockerfile (par exemple, `golang:1.20`) est la même que celle que vous avez utilisée pour créer votre application.

```
FROM golang:1.20.2-alpine3.16 as build
WORKDIR /helloworld
# Copy dependencies list
COPY go.mod go.sum ./
# Build
```

```
COPY main.go .
RUN go build -o main main.go
# Copy artifacts to a clean image
FROM alpine:3.16
COPY --from=build /helloworld/main /main
ENTRYPOINT [ "/main" ]
```

6. Générez l'image Docker à l'aide de la commande docker build. L'exemple suivant nomme l'image `docker-image` et lui donne la balise `test`. Pour rendre votre image compatible avec Lambda, vous devez utiliser l'option `--provenance=false`.

```
docker buildx build --platform linux/amd64 --provenance=false -t docker-image:test
 .
```

> **Note**
>
> La commande spécifie l'option `--platform linux/amd64` pour garantir la compatibilité de votre conteneur avec l'environnement d'exécution Lambda, quelle que soit l'architecture de votre machine de génération. Si vous avez l'intention de créer une fonction Lambda à l'aide de l'architecture du jeu d'instructions ARM64, veillez à modifier la commande pour utiliser plutôt l'option `--platform linux/arm64`.

(Facultatif) Testez l'image localement

Utilisez l'émulateur d'interface d'exécution pour tester l'image localement. Vous pouvez intégrer l'émulateur dans votre image ou utiliser la procédure suivante pour l'installer sur votre machine locale.

Pour installer et exécuter l'émulateur d'interface d'exécution sur votre ordinateur local

1. Depuis le répertoire de votre projet, exécutez la commande suivante pour télécharger l'émulateur d'interface d'exécution (architecture x86-64) GitHub et l'installer sur votre machine locale.

   Linux/macOS

```
mkdir -p ~/.aws-lambda-rie && \
    curl -Lo ~/.aws-lambda-rie/aws-lambda-rie https://github.com/aws/aws-lambda-
runtime-interface-emulator/releases/latest/download/aws-lambda-rie && \
    chmod +x ~/.aws-lambda-rie/aws-lambda-rie
```

Pour installer l'émulateur arm64, remplacez l'URL du GitHub référentiel dans la commande précédente par la suivante :

```
https://github.com/aws/aws-lambda-runtime-interface-emulator/releases/latest/
download/aws-lambda-rie-arm64
```

PowerShell

```
$dirPath = "$HOME\.aws-lambda-rie"
if (-not (Test-Path $dirPath)) {
    New-Item -Path $dirPath -ItemType Directory
}

$downloadLink = "https://github.com/aws/aws-lambda-runtime-interface-emulator/
releases/latest/download/aws-lambda-rie"
$destinationPath = "$HOME\.aws-lambda-rie\aws-lambda-rie"
Invoke-WebRequest -Uri $downloadLink -OutFile $destinationPath
```

Pour installer l'émulateur arm64, remplacez `$downloadLink` par ce qui suit :

```
https://github.com/aws/aws-lambda-runtime-interface-emulator/releases/latest/
download/aws-lambda-rie-arm64
```

2. Démarrez votre image Docker à l'aide de la commande docker run. Notez ce qui suit :

- `docker-image` est le nom de l'image et `test` est la balise.
- `/main` est le `ENTRYPOINT` de votre Dockerfile.

Linux/macOS

```
docker run --platform linux/amd64 -d -v ~/.aws-lambda-rie:/aws-lambda -p
 9000:8080 \
    --entrypoint /aws-lambda/aws-lambda-rie \
    docker-image:test \
        /main
```

PowerShell

```
docker run --platform linux/amd64 -d -v "$HOME\.aws-lambda-rie:/aws-lambda" -p
 9000:8080 `
--entrypoint /aws-lambda/aws-lambda-rie `
docker-image:test `
    /main
```

Cette commande exécute l'image en tant que conteneur et crée un point de terminaison local à `localhost:9000/2015-03-31/functions/function/invocations`.

> **Note**
>
> Si vous avez créé l'image Docker pour l'architecture du jeu d'instructions ARM64, veillez à utiliser l'option `--platform linux/arm64` plutôt que `--platform linux/amd64`.

3. Publiez un événement au point de terminaison local.

Linux/macOS

Sous Linux et macOS, exécutez la commande `curl` suivante :

```
curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d '{}'
```

Cette commande invoque la fonction avec un événement vide et renvoie une réponse. Si vous utilisez votre propre code de fonction plutôt que l'exemple de code de fonction, vous pouvez invoquer la fonction avec une charge utile JSON. Exemple :

```
curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d
 '{"payload":"hello world!"}'
```

PowerShell

Dans PowerShell, exécutez la `Invoke-WebRequest` commande suivante :

```
Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/
invocations" -Method Post -Body '{}' -ContentType "application/json"
```

Cette commande invoque la fonction avec un événement vide et renvoie une réponse. Si vous utilisez votre propre code de fonction plutôt que l'exemple de code de fonction, vous pouvez invoquer la fonction avec une charge utile JSON. Exemple :

```
Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/
invocations" -Method Post -Body '{"payload":"hello world!"}' -ContentType
 "application/json"
```

4. Obtenez l'ID du conteneur.

```
docker ps
```

5. Utilisez la commande docker kill pour arrêter le conteneur. Dans cette commande, remplacez `3766c4ab331c` par l'ID du conteneur de l'étape précédente.

```
docker kill 3766c4ab331c
```

Déploiement de l'image

Pour charger l'image sur Amazon RIE et créer la fonction Lambda

1. Exécutez la commande get-login-password pour authentifier la CLI Docker auprès de votre registre Amazon ECR.
   - Définissez la `--region` valeur à l' Région AWS endroit où vous souhaitez créer le référentiel Amazon ECR.
   - `111122223333`Remplacez-le par votre Compte AWS identifiant.

```
aws ecr get-login-password --region us-east-1 | docker login --username AWS --
password-stdin 111122223333.dkr.ecr.us-east-1.amazonaws.com
```

2. Créez un référentiel dans Amazon ECR à l'aide de la commande create-repository.

```
aws ecr create-repository --repository-name hello-world --region us-east-1 --image-
scanning-configuration scanOnPush=true --image-tag-mutability MUTABLE
```

> **Note**
>
> Le référentiel Amazon ECR doit être Région AWS identique à la fonction Lambda.

En cas de succès, vous obtenez une réponse comme celle-ci :

```
{
    "repository": {
        "repositoryArn": "arn:aws:ecr:us-east-1:111122223333:repository/hello-
world",
        "registryId": "111122223333",
        "repositoryName": "hello-world",
        "repositoryUri": "111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-
world",
        "createdAt": "2023-03-09T10:39:01+00:00",
        "imageTagMutability": "MUTABLE",
        "imageScanningConfiguration": {
            "scanOnPush": true
        },
        "encryptionConfiguration": {
            "encryptionType": "AES256"
        }
    }
}
```

3. Copiez le `repositoryUri` à partir de la sortie de l'étape précédente.
4. Exécutez la commande docker tag pour étiqueter votre image locale dans votre référentiel Amazon ECR en tant que dernière version. Dans cette commande :

   - `docker-image:test` est le nom et la balise de votre image Docker. Il s'agit du nom et de la balise de l'image que vous avez spécifiés dans la commande `docker build`.
   - Remplacez <ECRrepositoryUri> par l'`repositoryUri` que vous avez copié. Assurez-vous d'inclure `:latest` à la fin de l'URI.

```
docker tag docker-image:test <ECRrepositoryUri>:latest
```

Exemple :

```
docker tag docker-image:test 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

5. Exécutez la commande docker push pour déployer votre image locale dans le référentiel Amazon ECR. Assurez-vous d'inclure `:latest` à la fin de l'URI du référentiel.

```
docker push 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

6. Créez un rôle d'exécution pour la fonction, si vous n'en avez pas déjà un. Vous aurez besoin de l'Amazon Resource Name (ARN) du rôle à l'étape suivante.
7. Créez la fonction Lambda. Pour `ImageUri`, indiquez l'URI du référentiel mentionné précédemment. Assurez-vous d'inclure `:latest` à la fin de l'URI.

```
aws lambda create-function \
  --function-name hello-world \
  --package-type Image \
  --code ImageUri=111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \
  --role arn:aws:iam::111122223333:role/lambda-ex
```

> **Note**
>
> Vous pouvez créer une fonction en utilisant une image d'un autre AWS compte, à condition que l'image se trouve dans la même région que la fonction Lambda. Pour plus d'informations, consultez Autorisations entre comptes Amazon ECR.

8. Invoquer la fonction.

```
aws lambda invoke --function-name hello-world response.json
```

Vous devriez obtenir une réponse comme celle-ci :

```
{
  "ExecutedVersion": "$LATEST",
  "StatusCode": 200
}
```

9. Pour voir la sortie de la fonction, consultez le fichier `response.json`.

Pour mettre à jour le code de la fonction, vous devez recréer l'image, charger la nouvelle image dans le référentiel Amazon ECR, puis utiliser la commande update-function-code pour déployer l'image dans la fonction Lambda.

Lambda résout l'étiquette d'image en hachage d'image spécifique. Cela signifie que si vous pointez la balise d'image qui a été utilisée pour déployer la fonction vers une nouvelle image dans Amazon ECR, Lambda ne met pas automatiquement à jour la fonction pour utiliser la nouvelle image.

Pour déployer la nouvelle image sur la même fonction Lambda, vous devez utiliser la commande update-function-code, même si la balise d'image dans Amazon ECR reste la même. Dans l'exemple suivant, l'option `--publish` crée une version de la fonction à l'aide de l'image du conteneur mise à jour.

```
aws lambda update-function-code \
  --function-name hello-world \
  --image-uri 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \
  --publish
```

Utilisation de couches pour les fonctions d'événement Go Lambda

Nous déconseillons d’utiliser des couches pour gérer les dépendances des fonctions Lambda écrites en Go. Cela est dû au fait que les fonctions Lambda en Go sont compilées en un seul exécutable, que vous fournissez à Lambda lorsque vous déployez votre fonction. Cet exécutable contient votre code de fonction compilé, ainsi que toutes ses dépendances. L’utilisation de couches complique non seulement ce processus, mais entraîne également une augmentation des temps de démarrage à froid, car vos fonctions doivent charger manuellement des assemblages supplémentaires en mémoire pendant la phase d’initialisation.

Pour utiliser des dépendances externes avec vos gestionnaires Go, incluez-les directement dans votre package de déploiement. Ce faisant, vous simplifiez le processus de déploiement et profitez des optimisations du compilateur Go intégré. Pour un exemple d’importation et d’utilisation d’une dépendance telle que le kit SDK AWS pour Go dans votre fonction, consultez the section called “Handler (Gestionnaire)”.

Enregistrez et surveillez les fonctions des événements Go Lambda

AWS Lambda surveille automatiquement les fonctions d'événement Lambda en votre nom et envoie les journaux à Amazon. CloudWatch Votre fonction est fournie avec un groupe de CloudWatch journaux Logs et un flux de journaux pour chaque instance de votre fonction. L'environnement d'exécution Lambda envoie des informations sur chaque invocation au flux de journaux et transmet les journaux et autres sorties provenant du code de votre fonction. Pour plus d'informations, consultez Envoi des journaux des fonctions d'événements Lambda aux journaux CloudWatch.

Cette page explique comment générer une sortie de journal à partir du code de votre fonction Lambda et comment accéder aux journaux à l'aide de la AWS Command Line Interface console Lambda ou de la console. CloudWatch

Sections

- Création d'une fonction qui renvoie des journaux
- Affichage des journaux dans la console Lambda
- Afficher les journaux dans la CloudWatch console
- Afficher les journaux à l'aide du AWS Command Line Interface (AWS CLI)
- Suppression de journaux

Création d'une fonction qui renvoie des journaux

Pour générer les journaux à partir de votre code de fonction, vous pouvez utiliser des méthodes sur le package fmt ou n'importe quelle bibliothèque de journalisation qui écrit dans `stdout` ou `stderr`. L'exemple suivant utilise le package de journal.

Example main.go — Journalisation

```
func handleRequest(ctx context.Context, event events.SQSEvent) (string, error) {
  // event
  eventJson, _ := json.MarshalIndent(event, "", "  ")
  log.Printf("EVENT: %s", eventJson)
  // environment variables
  log.Printf("REGION: %s", os.Getenv("AWS_REGION"))
  log.Println("ALL ENV VARS:")
  for _, element := range os.Environ() {
    log.Println(element)
  }
```

Example format des journaux

```
START RequestId: dbda340c-xmpl-4031-8810-11bb609b4c71 Version: $LATEST
2020/03/27 03:40:05 EVENT: {
  "Records": [
    {
      "messageId": "19dd0b57-b21e-4ac1-bd88-01bbb068cb78",
      "receiptHandle": "MessageReceiptHandle",
      "body": "Hello from SQS!",
      "md5OfBody": "7b27xmplb47ff90a553787216d55d91d",
      "md5OfMessageAttributes": "",
      "attributes": {
        "ApproximateFirstReceiveTimestamp": "1523232000001",
        "ApproximateReceiveCount": "1",
        "SenderId": "123456789012",
        "SentTimestamp": "1523232000000"
      },
      ...
2020/03/27 03:40:05 AWS_LAMBDA_LOG_STREAM_NAME=2020/03/27/
[$LATEST]569cxmplc3c34c7489e6a97ad08b4419
2020/03/27 03:40:05 AWS_LAMBDA_FUNCTION_NAME=blank-go-function-9DV3XMPL6XBC
2020/03/27 03:40:05 AWS_LAMBDA_FUNCTION_MEMORY_SIZE=128
2020/03/27 03:40:05 AWS_LAMBDA_FUNCTION_VERSION=$LATEST
2020/03/27 03:40:05 AWS_EXECUTION_ENV=AWS_Lambda_go1.x
END RequestId: dbda340c-xmpl-4031-8810-11bb609b4c71
REPORT RequestId: dbda340c-xmpl-4031-8810-11bb609b4c71 Duration: 38.66 ms Billed
 Duration: 243 ms Memory Size: 128 MB Max Memory Used: 54 MB Init Duration: 203.69 ms
XRAY TraceId: 1-5e7d7595-212fxmpl9ee07c4884191322 SegmentId: 42ffxmpl0645f474 Sampled:
 true
```

L’environnement d’exécution Go enregistre les lignes `START`, `END` et `REPORT` pour chaque invocation. La ligne de rapport fournit les détails suivants.

Champs de données de la ligne REPORT

- RequestId— L'identifiant de demande unique pour l'invocation.
- Duration – Temps que la méthode de gestion du gestionnaire de votre fonction a consacré au traitement de l’événement.
- Billed Duration : temps facturé pour l’invocation.
- Memory Size – Quantité de mémoire allouée à la fonction.

- Max Memory Used – Quantité de mémoire utilisée par la fonction. Lorsque les appels partagent un environnement d'exécution, Lambda indique la mémoire maximale utilisée pour toutes les invocations. Ce comportement peut entraîner une valeur signalée plus élevée que prévu.
- Init Duration : pour la première requête servie, temps qu'il a pris à l'exécution charger la fonction et exécuter le code en dehors de la méthode du gestionnaire.
- XRAY TraceId — Pour les demandes suivies, l'ID de AWS X-Ray trace.
- SegmentId— Pour les demandes suivies, l'ID X-Ray du segment.
- Sampled – Pour les demandes suivies, résultat de l'échantillonnage.

Affichage des journaux dans la console Lambda

Vous pouvez utiliser la console Lambda pour consulter les résultats du journal après avoir invoqué une fonction d'événement Lambda.

Si votre code peut être testé à partir de l'éditeur de code intégré, vous trouverez des journaux dans les résultats d'exécution. Lorsque vous utilisez la fonctionnalité de test de la console pour appeler une fonction, vous trouverez la sortie du journal dans la section Détails.

Afficher les journaux dans la CloudWatch console

Vous pouvez utiliser la CloudWatch console Amazon pour consulter les journaux de toutes les invocations de la fonction d'événement Lambda.

Pour afficher les journaux sur la CloudWatch console

1. Ouvrez la page Groupes de journaux sur la CloudWatch console.
2. Choisissez le groupe de journaux pour votre fonction (/aws/lambda/***your-function-name***).
3. Choisissez un flux de journaux.

Chaque flux de journal correspond à une instance de votre fonction. Un flux de journal apparaît lorsque vous mettez à jour votre fonction Lambda et lorsque des instances supplémentaires sont créées pour gérer les appels simultanés. Pour trouver les journaux d'un appel spécifique, nous vous recommandons d'instrumenter votre fonction avec. AWS X-Ray X-Ray enregistre les détails de la demande et du flux de log dans le traçage.

Afficher les journaux à l'aide du AWS Command Line Interface (AWS CLI)

AWS CLI Il s'agit d'un outil open source que vous pouvez utiliser pour interagir avec les AWS services à l'aide de commandes dans votre interface de ligne de commande. Pour effectuer les étapes de cette section, vous devez disposer de la version 2 de l'AWS CLI.

Vous pouvez utiliser AWS CLI pour récupérer les journaux d'une invocation à l'aide de l'option de commande `--log-type`. La réponse inclut un champ `LogResult` qui contient jusqu'à 4 Ko de journaux codés en base64 provenant de l'invocation.

Example récupérer un ID de journal

L'exemple suivant montre comment récupérer un ID de journal à partir du champ `LogResult` d'une fonction nommée `my-function`.

```
aws lambda invoke --function-name my-function out --log-type Tail
```

Vous devriez voir la sortie suivante:

```
{
    "StatusCode": 200,
    "LogResult":
 "U1RBUlQgUmVxdWVzdElkOiA4N2QwNDRiOC1mMTU0LTExZTgtOGNkYS0yOTc0YzVlNGZiMjEgVmVyc2lvb...",
    "ExecutedVersion": "$LATEST"
}
```

Example décoder les journaux

Dans la même invite de commandes, utilisez l'utilitaire `base64` pour décoder les journaux. L'exemple suivant montre comment récupérer les journaux encodés en base64 pour `my-function`.

```
aws lambda invoke --function-name my-function out --log-type Tail \
--query 'LogResult' --output text --cli-binary-format raw-in-base64-out | base64 --
decode
```

L'cli-binary-formatoption est obligatoire si vous utilisez AWS CLI la version 2. Pour faire de ce paramètre le paramètre par défaut, exécutez `aws configure set cli-binary-format raw-in-base64-out`. Pour plus d'informations, consultez les options de ligne de commande globales AWS CLI prises en charge dans le Guide de l'utilisateur AWS Command Line Interface version 2.

Vous devriez voir la sortie suivante :

```
START RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8 Version: $LATEST
"AWS_SESSION_TOKEN": "AgoJb3JpZ2luX2VjELj...", "_X_AMZN_TRACE_ID": "Root=1-5d02e5ca-
f5792818b6fe8368e5b51d50;Parent=191db58857df8395;Sampled=0"",ask/lib:/opt/lib",
END RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8
REPORT RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8  Duration: 79.67 ms      Billed
 Duration: 80 ms         Memory Size: 128 MB     Max Memory Used: 73 MB
```

L'utilitaire `base64` est disponible sous Linux, macOS et Ubuntu sous Windows. Les utilisateurs de macOS auront peut-être besoin d'utiliser `base64 -D`.

Example Script get-logs.sh

Dans la même invite de commandes, utilisez le script suivant pour télécharger les cinq derniers événements de journalisation. Le script utilise `sed` pour supprimer les guillemets du fichier de sortie et attend 15 secondes pour permettre la mise à disposition des journaux. La sortie comprend la réponse de Lambda, ainsi que la sortie de la commande `get-log-events`.

Copiez le contenu de l'exemple de code suivant et enregistrez-le dans votre répertoire de projet Lambda sous `get-logs.sh`.

L'cli-binary-formatoption est obligatoire si vous utilisez AWS CLI la version 2. Pour faire de ce paramètre le paramètre par défaut, exécutez `aws configure set cli-binary-format raw-in-base64-out`. Pour plus d'informations, consultez les options de ligne de commande globales AWS CLI prises en charge dans le Guide de l'utilisateur AWS Command Line Interface version 2.

```
#!/bin/bash
aws lambda invoke --function-name my-function --cli-binary-format raw-in-base64-out --
payload '{"key": "value"}' out
sed -i'' -e 's/"//g' out
sleep 15
aws logs get-log-events --log-group-name /aws/lambda/my-function --log-stream-
name stream1 --limit 5
```

Example macOS et Linux (uniquement)

Dans la même invite de commande, les utilisateurs de macOS et de Linux devront peut-être exécuter la commande suivante pour s'assurer que le script est exécutable.

```
chmod -R 755 get-logs.sh
```

Example récupérer les cinq derniers événements de journal

Dans la même invite de commande, exécutez le script suivant pour obtenir les cinq derniers événements de journalisation.

```
./get-logs.sh
```

Vous devriez voir la sortie suivante:

```
{
    "StatusCode": 200,
    "ExecutedVersion": "$LATEST"
}
{
    "events": [
        {
            "timestamp": 1559763003171,
            "message": "START RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf Version:
 $LATEST\n",
            "ingestionTime": 1559763003309
        },
        {
            "timestamp": 1559763003173,
            "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tENVIRONMENT VARIABLES\r{\r  \"AWS_LAMBDA_FUNCTION_VERSION\": \"$LATEST\",
\r ...",
            "ingestionTime": 1559763018353
        },
        {
            "timestamp": 1559763003173,
            "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tEVENT\r{\r  \"key\": \"value\"\r}\n",
            "ingestionTime": 1559763018353
        },
        {
            "timestamp": 1559763003218,
            "message": "END RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf\n",
            "ingestionTime": 1559763018353
        },
        {
            "timestamp": 1559763003218,
```

```
            "message": "REPORT RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tDuration: 26.73 ms\tBilled Duration: 27 ms \tMemory Size: 128 MB\tMax Memory Used: 75
 MB\t\n",
            "ingestionTime": 1559763018353
        }
    ],
    "nextForwardToken": "f/34783877304859518393868359594929986069206639495374241795",
    "nextBackwardToken": "b/34783877303811383369537420289090800615709599058929582080"
}
```

Suppression de journaux

Les groupes de journaux ne sont pas supprimés automatiquement quand vous supprimez une fonction. Pour éviter de stocker des journaux indéfiniment, supprimez le groupe de journaux ou configurez une période de conservation à l'issue de laquelle les journaux sont supprimés automatiquement.

Instrumentation du code Go AWS Lambda

Lambda s'intègre pour vous aider AWS X-Ray à suivre, à déboguer et à optimiser les applications Lambda. Vous pouvez l'utiliser X-Ray pour suivre une demande lorsqu'elle parcourt les ressources de votre application, ce qui peut inclure des fonctions Lambda et AWS d'autres services.

Pour envoyer des données de suivi à X-Ray, vous pouvez utiliser l'une des deux bibliothèques du SDK :

- AWS Distro for OpenTelemetry (ADOT) — Une distribution sécurisée, prête pour la production et prise AWS en charge du SDK (OTel). OpenTelemetry
- AWS X-Ray SDK for Go : SDK permettant de générer et d'envoyer des données de suivi à. X-Ray

Chacun des SDK propose des moyens d'envoyer vos données de télémétrie au service. X-Ray Vous pouvez ensuite les utiliser X-Ray pour afficher, filtrer et obtenir des informations sur les indicateurs de performance de votre application afin d'identifier les problèmes et les opportunités d'optimisation.

> **Important**
>
> Les X-Ray et Powertools for AWS Lambda SDK font partie d'une solution d'instrumentation étroitement intégrée proposée par. AWS Les couches ADOT Lambda font partie d'une norme industrielle pour l'instrumentation de traçage qui collecte plus de données en général, mais qui peut ne pas convenir à tous les cas d'utilisation. Vous pouvez implémenter le suivi de bout en bout à l' X-Ray aide de l'une ou l'autre solution. Pour en savoir plus sur le choix entre les deux, voir Choisir entre la AWS distribution pour Open Telemetry et les SDK. X-Ray

Sections

- Utilisation d'ADOT pour instrumenter vos fonctions Go
- Utiliser le X-Ray SDK pour instrumenter vos fonctions Go
- Activation du suivi avec la console Lambda
- Activation du suivi avec l'API Lambda
- Activation du traçage avec CloudFormation
- Interprétation et X-Ray traçage

Utilisation d'ADOT pour instrumenter vos fonctions Go

ADOT fournit des couches Lambda entièrement gérées qui regroupent tout ce dont vous avez besoin pour collecter des données de télémétrie à l'aide du kit SDK OTel. En consommant cette couche, vous pouvez instrumenter vos fonctions Lambda sans avoir à modifier le code de fonction. Vous pouvez également configurer votre couche pour effectuer une initialisation personnalisée d'OTel. Pour de plus amples informations, veuillez consulter Configuration personnalisée pour ADOT Collector sur Lambda dans la documentation ADOT.

Pour les exécutions python, vous pouvez ajouter la AWS couche Lambda gérée pour ADOT Go pour instrumenter automatiquement vos fonctions. Pour obtenir des instructions détaillées sur la façon d'ajouter cette couche, consultez AWS Distro for OpenTelemetry Lambda Support for Go dans la documentation ADOT. Pour obtenir des instructions sur la conversion des événements de l'API de télémétrie Lambda en spans, consultez. OpenTelemetry the section called "Conversion d'événements en OTel Spans"

Utiliser le X-Ray SDK pour instrumenter vos fonctions Go

Pour enregistrer les détails des appels que votre fonction Lambda effectue vers d'autres ressources de votre application, vous pouvez également utiliser le AWS X-Ray SDK for Go. Pour obtenir le SDK, téléchargez-le depuis son GitHub dépôt avec : `go get`

```
go get github.com/aws/aws-xray-sdk-go
```

Pour instrumenter les clients du AWS SDK, transmettez-les à la `xray.AWS()` méthode. Ensuite, vous pouvez suivre vos appels à l'aide de la version `WithContext` de la méthode.

```
svc := s3.New(session.New())
xray.AWS(svc.Client)
...
svc.ListBucketsWithContext(ctx aws.Context, input *ListBucketsInput)
```

Après avoir ajouté les bonnes dépendances et apporté les modifications de code nécessaires, activez le suivi dans la configuration de votre fonction via la console Lambda ou l'API.

Activation du suivi avec la console Lambda

Pour activer le suivi actif de votre fonction d'événement Lambda à l'aide de la console, procédez comme suit :

Pour activer le traçage actif

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez une fonction d'événement.
3. Choisissez Configuration, puis choisissez Outils de surveillance et d'opérations.
4. Dans Outils de surveillance supplémentaires, choisissez Modifier.
5. Sous Signaux CloudWatch d'application et AWS X-Ray sélectionnez Activer les traces de service Lambda.
6. Cliquez sur Enregistrer.

Activation du suivi avec l'API Lambda

Configurez le suivi sur votre fonction Lambda avec le AWS SDK AWS CLI or, utilisez les opérations d'API suivantes :

- UpdateFunctionConfiguration
- GetFunctionConfiguration
- CreateFunction

L'exemple de AWS CLI commande suivant active le suivi actif sur une fonction nommée my-function.

```
aws lambda update-function-configuration --function-name my-function \
--tracing-config Mode=Active
```

Le mode de suivi fait partie de la configuration spécifique de la version lorsque vous publiez une version de votre fonction. Vous ne pouvez pas modifier le mode de suivi sur une version publiée.

Activation du traçage avec CloudFormation

Pour activer le suivi d'une `AWS::Lambda::Function` ressource dans un CloudFormation modèle, utilisez la `TracingConfig` propriété.

Example fonction-inline.yml — Configuration du suivi

```
Resources:
  function:
```

```
    Type: AWS::Lambda::Function
    Properties:
      TracingConfig:
        Mode: Active
      ...
```

Pour une `AWS::Serverless::Function` ressource AWS Serverless Application Model (AWS SAM), utilisez la `Tracing` propriété.

Example template.yml — Configuration du suivi

```
Resources:
  function:
    Type: AWS::Serverless::Function
    Properties:
      Tracing: Active
      ...
```

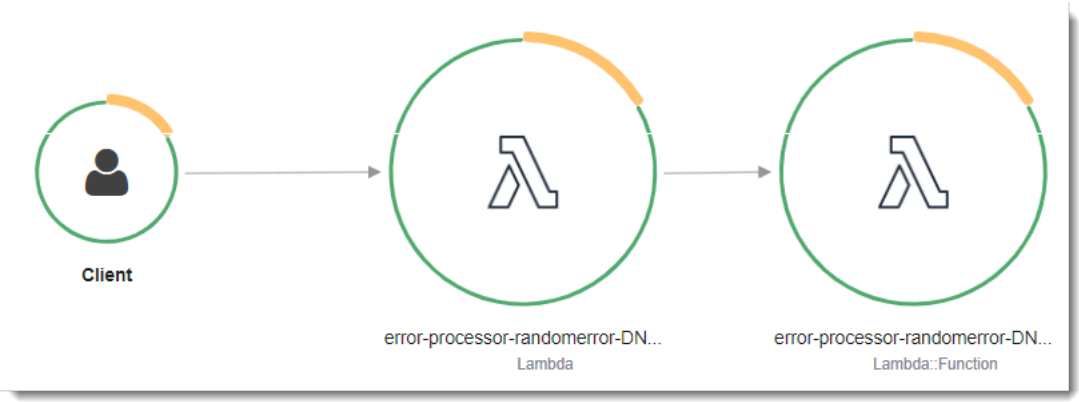
Interprétation et X-Ray traçage

Votre fonction événementielle a besoin d'une autorisation pour télécharger des données de suivi sur X-Ray. Lorsque vous activez le suivi dans la console Lambda, Lambda ajoute les autorisations requises au rôle d'exécution de votre fonction d'événement. Dans le cas contraire, ajoutez la AWSXRayDaemonWriteAccesspolitique au rôle d'exécution.

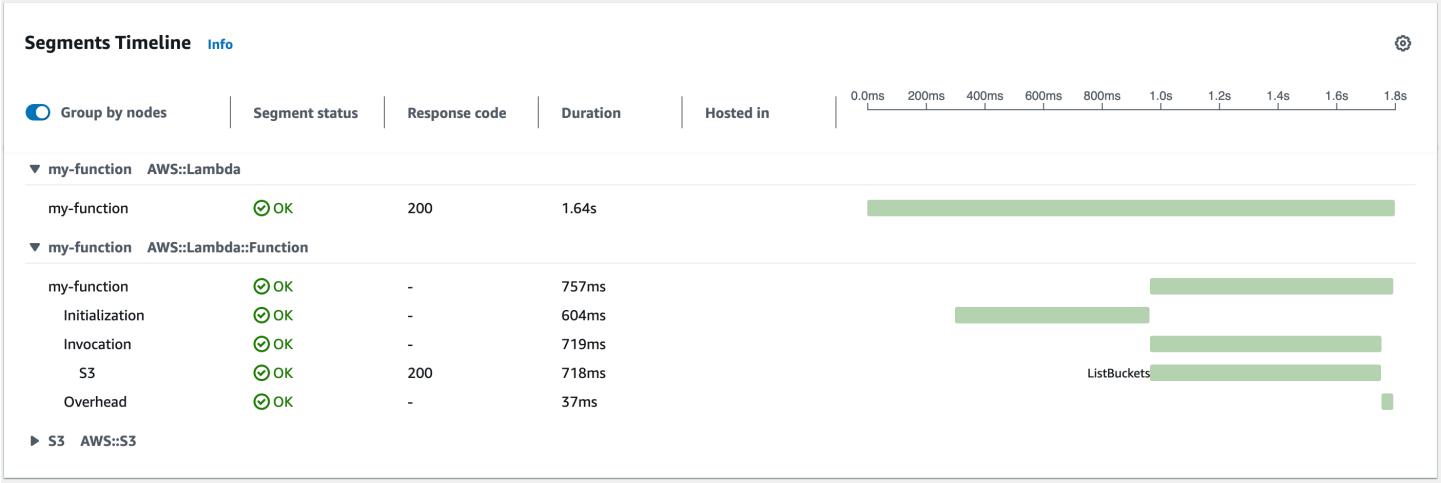
Une fois que vous avez configuré le suivi actif, vous pouvez observer des demandes spécifiques via votre application. Le graphique X-Ray de service affiche des informations sur votre application et tous ses composants. L'exemple suivant montre une application dotée de deux fonctions. La fonction principale traite les événements et renvoie parfois des erreurs. La deuxième fonction située en haut traite les erreurs qui apparaissent dans le groupe de journaux de la première et utilise le AWS SDK pour appeler X-Ray Amazon Simple Storage Service (Amazon S3) et Amazon Logs. CloudWatch

X-Ray ne retrace pas toutes les demandes jusqu'à votre application. X-Ray applique un algorithme d'échantillonnage pour garantir l'efficacité du suivi, tout en fournissant un échantillon représentatif de toutes les demandes. Le taux d'échantillonnage est 1 demande par seconde et 5 % de demandes supplémentaires. Vous ne pouvez pas configurer le taux X-Ray d'échantillonnage pour vos fonctions.

Dans X-Ray, un suivi enregistre des informations relatives à une demande traitée par un ou plusieurs services. Lambda enregistre deux segments par suivi, ce qui a pour effet de créer deux nœuds sur le graphique du service. L'image suivante met en évidence ces deux nœuds :



Le premier nœud sur la gauche représente le service Lambda qui reçoit la demande d'invocation. Le deuxième nœud représente votre fonction Lambda spécifique. L'exemple suivant illustre une trace avec ces deux segments. Les deux sont nommés my-function, mais l'un a pour origine `AWS::Lambda` et l'autre a pour origine `AWS::Lambda::Function`. Si le segment `AWS::Lambda` affiche une erreur, cela signifie que le service Lambda a rencontré un problème. Si le segment `AWS::Lambda::Function` affiche une erreur, cela signifie que votre fonction a rencontré un problème.



Cet exemple développe le segment `AWS::Lambda::Function` pour afficher ses trois sous-segments.

> **Note**
>
> AWS met actuellement en œuvre des modifications du service Lambda. En raison de ces modifications, vous pouvez constater des différences mineures entre la structure et le contenu des messages du journal système et des segments de trace émis par les différentes fonctions d'événement Lambda de votre ordinateur. Compte AWS
> L'exemple de suivi présenté ici illustre le segment de fonction à l'ancienne. Les différences entre les segments à l'ancienne et de style moderne sont décrites dans les paragraphes suivants.
> Ces modifications seront mises en œuvre au cours des prochaines semaines, et toutes les fonctions, Régions AWS sauf en Chine et dans les GovCloud régions, seront transférées pour utiliser le nouveau format des messages de journal et des segments de trace.

Le segment de fonction à l'ancienne contient les sous-segments suivants :

- Initialization (Initialisation) : représente le temps passé à charger votre fonction et à exécuter le code d'initialisation. Ce sous-segment apparaît pour le premier événement traité par chaque instance de votre fonction.
- Invocation – Représente le temps passé à exécuter votre code de gestionnaire.
- Overhead (Travail supplémentaire) – Représente le temps que le fichier d'exécution Lambda passe à se préparer à gérer l'événement suivant.

Le segment de fonction de style moderne ne contient pas de sous-segment `Invocation`. À la place, les sous-segments du client sont directement rattachés au segment de fonction. Pour plus d'informations sur la structure des segments de fonction à l'ancienne et de style moderne, consultez the section called “Comprendre les X-Ray traces”.

Vous pouvez également utiliser des clients HTTP, enregistrer des requêtes SQL et créer des sous-segments personnalisés avec des annotations et des métadonnées. Pour plus d'informations, consultez AWS X-Ray Kit SDK X-Ray pour Go dans le AWS X-Ray Guide du développeur.

> **Tarification**
>
> Vous pouvez utiliser le X-Ray suivi gratuitement chaque mois jusqu'à une certaine limite dans le cadre du niveau AWS gratuit. Au-delà de ce seuil, les X-Ray frais de stockage et de récupération des traces sont facturés. Pour en savoir plus, consultez Pricing AWS X-Ray (Tarification).

Création de fonctions d'événement Lambda avec C#

Vous pouvez exécuter votre application .NET en tant que fonction d'événement Lambda à l'aide du moteur d'exécution .NET 8 géré, d'un environnement d'exécution personnalisé ou d'une image de conteneur. Une fois le code de votre application compilé, vous pouvez le déployer dans Lambda sous la forme d'un fichier .zip ou d'une image de conteneur. Lambda fournit les exécutions suivantes pour les langages .NET :

Pour plus d'informations sur l'utilisation des couches .NET, consultezthe section called “Layers”. Pour obtenir des conseils sur le test de vos fonctions C#, consultezthe section called “Tests”.

Nom	Identifiant	Système d'exploitation	Date d'obsolescence	Créer la fonction de blocage	Mettre à jour la fonction de blocage
.NET 10	`dotnet10`	Amazon Linux 2	14 novembre 2028	14 déc. 2028	15 janvier 2029
.NET 9 (conteneur uniquement)	`dotnet9`	Amazon Linux 2	10 novembre 2026	Non planifié	Non planifié

Nom	Identifiant	Système d'exploitation	Date d'obsolescence	Créer la fonction de blocage	Mettre à jour la fonction de blocage
.NET 8	`dotnet8`	Amazon Linux 2	10 novembre 2026	29 juillet 2027	31 août 2027

Configuration de votre environnement de développement .NET

Pour développer et créer vos fonctions d'événement Lambda, vous pouvez utiliser n'importe quel environnement de développement intégré (IDE) .NET couramment disponible, notamment Microsoft Visual Studio, Visual Studio Code et JetBrains Rider. Pour simplifier votre expérience de développement, AWS fournit un ensemble de modèles de projets .NET, ainsi que l'interface de ligne de `Amazon.Lambda.Tools` commande (CLI).

Exécutez les commandes CLI .NET suivantes pour installer ces modèles de projet et ces outils de ligne de commande.

Installation des modèles de projet .NET

Pour installer les modèles de projet, exécutez la commande suivante :

```
dotnet new install Amazon.Lambda.Templates
```

Installation et mise à jour des outils CLI

Exécutez les commandes suivantes pour installer, mettre à jour ou désinstaller la CLI `Amazon.Lambda.Tools`.

Pour installer les outils de ligne de commande :

```
dotnet tool install -g Amazon.Lambda.Tools
```

Pour mettre à jour les outils de ligne de commande :

```
dotnet tool update -g Amazon.Lambda.Tools
```

Pour désinstaller les outils de ligne de commande :

```
dotnet tool uninstall -g Amazon.Lambda.Tools
```

Définir le gestionnaire de fonctions d'événement Lambda en C#

Le gestionnaire de fonctions d'événement Lambda est la méthode de votre code de fonction qui traite les événements. Lorsque votre fonction est invoquée, Lambda exécute la méthode du gestionnaire. Votre fonction s'exécute jusqu'à ce que le gestionnaire renvoie une réponse, se ferme ou expire.

Cette page explique comment utiliser les gestionnaires de fonctions d'événement Lambda en C# pour fonctionner avec l'environnement d'exécution géré .NET, y compris les options de configuration du projet, les conventions de dénomination et les meilleures pratiques. Cette page inclut également un exemple de fonction Lambda C# qui collecte des informations relatives à une commande, produit un reçu sous forme de fichier texte et place ce fichier dans un compartiment Amazon Simple Storage Service (S3). Pour plus d'informations sur le déploiement de votre fonction après l'avoir écrite, consultez the section called "Package de déploiement" ou the section called "Déploiement d'images de conteneur".

Rubriques

- Configuration de votre projet de gestionnaire C#
- Exemple de code de fonction d'événement Lambda en C#
- Gestionnaires de bibliothèques de classes
- Gestionnaires d'assemblages exécutables
- Signatures de gestionnaire valides pour les fonctions C#
- Convention de nommage du gestionnaire
- Sérialisation dans les fonctions d'événement Lambda en C#
- File-based fonctions
- Accès et utilisation de l'objet de contexte Lambda
- Utilisation de SDK pour .NET v3 dans votre gestionnaire
- Accès aux variables d'environnement
- Utilisation de l'état global
- Simplifiez le code de la fonction à l'aide du cadre d'annotations Lambda
- Meilleures pratiques en matière de code pour les fonctions d'événement Lambda en C#

Configuration de votre projet de gestionnaire C#

Lorsque vous utilisez les fonctions d'événement Lambda en C#, le processus consiste à écrire votre code, puis à le déployer sur Lambda. Il existe deux modèles de déploiement différents pour les

fonctions Lambda dans .NET : l'approche de la bibliothèque de classes et l'approche de l'assemblage exécutable.

Dans l'approche de bibliothèque de classes, vous empaquetez le code de votre fonction sous forme d'assemblage .NET (`.dll`) et le déployez sur Lambda avec l'environnement d'exécution géré .NET (`dotnet8`). Pour le nom du gestionnaire, Lambda attend une chaîne au format `AssemblyName::Namespace.Classname::Methodname`. Pendant la phase d'initialisation de la fonction, la classe de votre fonction est initialisée et tout code contenu dans le constructeur est exécuté.

Dans l'approche d'assemblage exécutable, vous utilisez la fonctionnalité d'instructions de haut niveau qui a été introduite pour la première fois avec C# 9. Cette approche génère un assemblage exécutable que Lambda exécute chaque fois qu'il reçoit une commande d'invocation pour votre fonction. Dans cette approche, vous utilisez également l'environnement d'exécution géré .NET (`dotnet8`). Pour le nom de gestionnaire, vous fournissez à Lambda le nom de l'assemblage exécutable à exécuter.

L'exemple principal de cette page illustre l'approche de bibliothèque de classes. Vous pouvez initialiser votre projet Lambda C# de différentes manières, mais la méthode la plus simple consiste à utiliser la CLI .NET avec `Amazon.Lambda.Tools` CLI. Configurez `Amazon.Lambda.Tools` CLI en suivant les étapes décrites dans the section called "Environnement de développement". Ensuite, initialisez votre projet avec la commande suivante :

```
dotnet new lambda.EmptyFunction --name ExampleCS
```

Cette commande génère la structure de fichiers suivante :

```
/project-root
    # src
        # ExampleCS
            # Function.cs (contains main handler)
            # Readme.md
            # aws-lambda-tools-defaults.json
            # ExampleCS.csproj
    # test
         # ExampleCS.Tests
            # FunctionTest.cs (contains main handler)
            # ExampleCS.Tests.csproj
```

Dans cette structure de fichiers, la logique du gestionnaire principal de votre fonction réside dans le fichier `Function.cs`.

Exemple de code de fonction d'événement Lambda en C#

L'exemple de code de fonction Lambda C# suivant prend en compte les informations relatives à une commande, produit un reçu sous forme de fichier texte et place ce fichier dans un compartiment Amazon S3.

Example **`Function.cs`**Fonction d'événement Lambda

```
using System;
using System.Text;
using System.Threading.Tasks;
using Amazon.Lambda.Core;
using Amazon.S3;
using Amazon.S3.Model;

// Assembly attribute to enable Lambda function logging
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSerializer

namespace ExampleLambda;

public class Order
{
    public string OrderId { get; set; } = string.Empty;
    public double Amount { get; set; }
    public string Item { get; set; } = string.Empty;
}

public class OrderHandler
{
    private static readonly AmazonS3Client s3Client = new();

    public async Task<string> HandleRequest(Order order, ILambdaContext context)
    {
        try
        {
            string? bucketName = Environment.GetEnvironmentVariable("RECEIPT_BUCKET");
            if (string.IsNullOrWhiteSpace(bucketName))
            {
```

```
                throw new ArgumentException("RECEIPT_BUCKET environment variable is not
 set");
            }

            string receiptContent = $"OrderID: {order.OrderId}\nAmount:
 ${order.Amount:F2}\nItem: {order.Item}";
            string key = $"receipts/{order.OrderId}.txt";

            await UploadReceiptToS3(bucketName, key, receiptContent);

            context.Logger.LogInformation($"Successfully processed order
 {order.OrderId} and stored receipt in S3 bucket {bucketName}");
            return "Success";
        }
        catch (Exception ex)
        {
            context.Logger.LogError($"Failed to process order: {ex.Message}");
            throw;
        }
    }

    private async Task UploadReceiptToS3(string bucketName, string key, string
 receiptContent)
    {
        try
        {
            var putRequest = new PutObjectRequest
            {
                BucketName = bucketName,
                Key = key,
                ContentBody = receiptContent,
                ContentType = "text/plain"
            };

            await s3Client.PutObjectAsync(putRequest);
        }
        catch (AmazonS3Exception ex)
        {
            throw new Exception($"Failed to upload receipt to S3: {ex.Message}", ex);
        }
    }
}
```

Ce fichier `Function.cs` comprend les sections suivantes :

- Instructions `using` : utilisez ces instructions pour importer les classes C# que votre fonction Lambda nécessite.
- `[assembly: LambdaSerializer(...)]` : `LambdaSerializer` est un attribut d'assemblage qui indique à Lambda de convertir automatiquement les données utiles des événements JSON en objets C# avant de les transmettre à votre fonction.
- `namespace ExampleLambda` : définit l'espace de noms. En C#, il n'est pas nécessaire que le nom de l'espace de noms corresponde au nom du fichier.
- `public class Order {...}` : définit la forme de l'événement d'entrée attendu.
- `public class OrderHandler {...}` : définit votre classe C#. Vous y définirez la méthode du gestionnaire principal ainsi que toutes autres méthodes auxiliaires.
- `private static readonly AmazonS3Client s3Client = new();` : initialise un client Amazon S3 avec la chaîne de fournisseur d'informations d'identification par défaut, en dehors de la méthode du gestionnaire principal. Cela oblige Lambda à exécuter ce code pendant la phase d'initialisation.
- `public async ... HandleRequest (Order order, ILambdaContext context)` : il s'agit de la méthode de gestion principale, qui contient la logique principale de votre application.
- `private async Task UploadReceiptToS3(...) {}` : il s'agit d'une méthode auxiliaire référencée par la méthode de gestion principale `handleRequest`.

Comme cette fonction nécessite un client SDK Amazon S3, vous devez l'ajouter aux dépendances de votre projet. Vous pouvez également le faire en accédant à `src/ExampleCS` et en exécutant la commande suivante :

```
dotnet add package AWSSDK.S3
```

Ajouter des informations de métadonnées à aws-lambda-tools-defaults.json

Par défaut, le fichier `aws-lambda-tools-defaults.json` généré ne contient aucune information `profile` ou `region` relative à votre fonction. Mettez également à jour la chaîne `function-handler` avec la bonne valeur (`ExampleCS::ExampleLambda.OrderHandler::HandleRequest`). Vous pouvez effectuer cette mise à jour manuellement et ajouter les métadonnées nécessaires pour utiliser un profil d'identification et une région spécifiques pour votre fonction. Par exemple, votre fichier `aws-lambda-tools-defaults.json` doit ressembler à ceci :

```
{
  "Information": [
    "This file provides default values for the deployment wizard inside Visual Studio
 and the AWS Lambda commands added to the .NET Core CLI.",
    "To learn more about the Lambda commands with the .NET Core CLI execute the
 following command at the command line in the project root directory.",
    "dotnet lambda help",
    "All the command line options for the Lambda command can be specified in this
 file."
  ],
  "profile": "default",
  "region": "us-east-1",
  "configuration": "Release",
  "function-architecture": "x86_64",
  "function-runtime": "dotnet8",
  "function-memory-size": 512,
  "function-timeout": 30,
  "function-handler": "ExampleCS::ExampleLambda.OrderHandler::HandleRequest"
}
```

Pour que cette fonction fonctionne correctement, son rôle d'exécution doit autoriser l'action `s3:PutObject`. Assurez-vous également de définir la variable d'environnement `RECEIPT_BUCKET`. Après une invocation réussie, le compartiment Amazon S3 doit contenir un fichier de reçu.

Gestionnaires de bibliothèques de classes

L'exemple de code principal de cette page illustre un gestionnaire de bibliothèques de classes. La structure des gestionnaires de bibliothèques de classes est la suivante :

```
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSerializer

namespace NAMESPACE;

...

public class CLASSNAME {
    public async Task<string> METHODNAME (...) {
    ...
    }
}
```

Lorsque vous créez une fonction d'événement Lambda, vous devez fournir à Lambda des informations sur le gestionnaire de votre fonction sous la forme d'une chaîne dans le champ Handler. Cette chaîne indique à Lambda quelle méthode de votre code doit être exécutée lorsque votre fonction est invoquée. En C#, pour les gestionnaires de bibliothèques de classes, le format de la chaîne du gestionnaire est `ASSEMBLY::TYPE::METHOD`, où :

- `ASSEMBLY` est le nom du fichier d'assemblage .NET de votre application. Si vous utilisez la CLI `Amazon.Lambda.Tools` pour créer votre application et que vous ne définissez pas le nom de l'assemblage à l'aide de la propriété `AssemblyName` dans le fichier `.csproj`, alors `ASSEMBLY` est simplement le nom de votre fichier `.csproj`.
- `TYPE` est le nom complet du type de gestionnaire, à savoir `NAMESPACE.CLASSNAME`.
- `METHOD` est le nom de la méthode de gestionnaire principale de fonction dans votre code, à savoir `METHODNAME`.

Dans l'exemple de code principal illustré sur cette page, si l'assemblage est nommé `ExampleCS`, alors la chaîne du gestionnaire complète est `ExampleCS::ExampleLambda.OrderHandler::HandleRequest`.

Gestionnaires d'assemblages exécutables

Vous pouvez également définir des fonctions Lambda en C# sous forme d'assemblage exécutable. Les gestionnaires d'assemblages exécutables utilisent la fonctionnalité d'instructions de haut niveau de C#, dans laquelle le compilateur génère la `Main()` méthode et y insère le code de votre fonction. Lors de l'utilisation d'assemblages exécutables, l'exécution Lambda doit être amorcée.

Pour ce faire, utilisez la méthode `LambdaBootstrapBuilder.Create` dans votre code. Les entrées de cette méthode sont la fonction principale du gestionnaire ainsi que le sérialiseur Lambda à utiliser. Voici un exemple de gestionnaire d'assemblages exécutables en C# :

```
namespace GetProductHandler;

IDatabaseRepository repo = new DatabaseRepository();

await LambdaBootstrapBuilder.Create<APIGatewayProxyRequest>(Handler, new
 DefaultLambdaJsonSerializer())
    .Build()
    .RunAsync();
```

```
async Task<APIGatewayProxyResponse> Handler(APIGatewayProxyRequest apigProxyEvent,
 ILambdaContext context)
{
    var id = apigProxyEvent.PathParameters["id"];
    var databaseRecord = await this.repo.GetById(id);

    return new APIGatewayProxyResponse
    {
        StatusCode = (int)HttpStatusCode.OK,
        Body = JsonSerializer.Serialize(databaseRecord)
    };
};
```

Dans le champ Gestionnaire pour les gestionnaires d'assemblages exécutables, la chaîne du gestionnaire qui indique à Lambda comment exécuter votre code est le nom de l'assemblage. Dans cet exemple, il s'agit de `GetProductHandler`.

Signatures de gestionnaire valides pour les fonctions C#

En C#, les signatures de gestionnaire Lambda valides prennent entre 0 et 2 arguments. Généralement, la signature de votre gestionnaire comporte deux arguments, comme indiqué dans l'exemple principal :

```
public async Task<string> HandleRequest(Order order, ILambdaContext context)
```

Lorsque vous fournissez deux arguments, le premier argument doit être l'entrée de l'événement et le second doit être l'objet de contexte Lambda. Les deux arguments sont facultatifs. Par exemple, les signatures de gestionnaire Lambda suivantes sont également valides en C# :

- `public async Task<string> HandleRequest()`
- `public async Task<string> HandleRequest(Order order)`
- `public async Task<string> HandleRequest(ILambdaContext context)`

Outre la syntaxe de base de la signature du gestionnaire, il existe un certain nombre de restrictions supplémentaires :

- Vous ne pouvez pas utiliser le mot clé `unsafe` dans la signature du gestionnaire. Cependant, vous pouvez utiliser le contexte `unsafe` dans la méthode du gestionnaire et ses dépendances. Pour de plus amples informations, veuillez consulterdangereux (référence C#)sur le site Web de documentation de Microsoft.

- Le gestionnaire ne peut pas utiliser le `params` mot-clé, ni l'utiliser `ArgIterator` comme paramètre d'entrée ou de retour. Ces mots clés prennent en charge un nombre variable de paramètres. Le nombre maximum d'arguments que votre gestionnaire peut accepter est de deux.
- Le gestionnaire ne peut pas être une méthode générique. En d'autres termes, il ne peut pas utiliser de paramètres de type générique, comme <T>.
- Lambda ne prend pas en charge les gestionnaires asynchrones contenant `async void` dans la signature.

Convention de nommage du gestionnaire

Les gestionnaires Lambda en C# ne sont pas soumis à des restrictions de dénomination strictes. Toutefois, vous devez vous assurer que vous fournissez la bonne chaîne de gestionnaire à Lambda lorsque vous déployez votre fonction. La bonne chaîne de gestionnaire varie selon que vous déployez un gestionnaire de bibliothèques de classes ou un gestionnaire d'assemblages exécutables.

Bien que vous puissiez utiliser n'importe quel nom pour votre gestionnaire, les noms de fonctions en C# sont généralement disponibles. PascalCase De plus, même si le nom du fichier ne doit pas nécessairement correspondre au nom de la classe ou au nom du gestionnaire, il est généralement recommandé d'utiliser un nom de fichier comme `OrderHandler.cs` si le nom de votre classe est `OrderHandler`. Dans cet exemple, vous pouvez modifier le nom de fichier de `Function.cs` à `OrderHandler.cs`.

Sérialisation dans les fonctions d'événement Lambda en C#

JSON est le format d'entrée le plus courant et le plus standard pour les fonctions d'événement Lambda. Dans cet exemple, la fonction exige une entrée similaire à l'exemple suivant :

```
{
    "orderId": "12345",
    "amount": 199.99,
    "item": "Wireless Headphones"
}
```

En C#, vous pouvez définir la forme de l'événement d'entrée attendu dans une classe. Dans cet exemple, nous définissons la classe `Order` pour modéliser cette entrée :

```
public class Order
{
```

```
    public string OrderId { get; set; } = string.Empty;
    public double Amount { get; set; }
    public string Item { get; set; } = string.Empty;
}
```

Si votre fonction Lambda utilise des types d'entrée ou de sortie autres qu'un objet `Stream`, vous devez ajouter une bibliothèque de sérialisation à votre application. Vous pouvez ensuite convertir l'entrée JSON en une instance de la classe que vous avez définie. Il existe deux méthodes de sérialisation pour les fonctions C# dans Lambda : la sérialisation basée sur la réflexion et la sérialisation générée par la source.

Reflection-based sérialisation

AWS fournit des bibliothèques prédéfinies que vous pouvez rapidement ajouter à votre application. Ces bibliothèques implémentent la sérialisation à l'aide de la réflexion. Utilisez l'un des packages suivants pour implémenter la sérialisation basée sur la réflexion :

- `Amazon.Lambda.Serialization.SystemTextJson` : dans le backend, ce package utilise `System.Text.Json` pour effectuer des tâches de sérialisation.
- `Amazon.Lambda.Serialization.Json` : dans le backend, ce package utilise `Newtonsoft.Json` pour effectuer des tâches de sérialisation.

Vous pouvez également créer votre propre bibliothèque de sérialisation en implémentant l'interface `ILambdaSerializer`, disponible dans la bibliothèque `Amazon.Lambda.Core`. Cette interface définit deux méthodes :

- `T Deserialize<T>(Stream requestStream);`

  Vous implémentez cette méthode afin de désérialiser la charge utile de la demande à partir de l'API `Invoke` dans l'objet qui est transféré à votre gestionnaire de fonction Lambda.
- `T Serialize<T>(T response, Stream responseStream);`

  Vous implémentez cette méthode pour sérialiser le résultat renvoyé à partir de votre gestionnaire de fonction Lambda dans la charge utile de la réponse renvoyée par l'opération d'API `Invoke`.

L'exemple principal de cette page utilise la sérialisation basée sur la réflexion. Reflection-based la sérialisation fonctionne immédiatement AWS Lambda et ne nécessite aucune configuration supplémentaire, ce qui en fait un bon choix pour des raisons de simplicité. Toutefois, elle nécessite

une utilisation plus importante de la mémoire de la fonction. Il est également possible que les latences des fonctions soient plus élevées en raison de la réflexion sur le temps d'exécution.

Source-generated sérialisation

Avec la sérialisation générée par la source, le code de sérialisation est généré au moment de la compilation. Cela supprime le besoin de réflexion et peut améliorer les performances de votre fonction. Pour utiliser la sérialisation générée par la source dans votre fonction, vous devez procéder comme suit :

- Créez une nouvelle classe partielle qui hérite de `JsonSerializerContext`, en ajoutant des attributs `JsonSerializable` pour tous les types qui nécessitent une sérialisation ou une désérialisation.
- Configurez le `LambdaSerializer` afin d'utiliser un `SourceGeneratorLambdaJsonSerializer<T>`.
- Mettez à jour toute sérialisation ou désérialisation manuelle dans le code de votre application afin d’utiliser la classe nouvellement créée.

L’exemple suivant montre comment vous pouvez modifier l’exemple principal de cette page, qui utilise la sérialisation basée sur la réflexion, pour utiliser plutôt la sérialisation générée par la source.

```
using System.Text.Json;
using System.Text.Json.Serialization;

...

public class Order
{
    public string OrderId { get; set; } = string.Empty;
    public double Amount { get; set; }
    public string Item { get; set; } = string.Empty;
}

[JsonSerializable(typeof(Order))]
public partial class OrderJsonContext : JsonSerializerContext {}

public class OrderHandler
{

    ...
```

```
    public async Task<string> HandleRequest(string input, ILambdaContext context)
    {

    var order = JsonSerializer.Deserialize(input, OrderJsonContext.Default.Order);

    ...

    }

}
```

Source-generated la sérialisation nécessite plus de configuration que la sérialisation basée sur la réflexion. Cependant, les fonctions utilisant la sérialisation générée par la source ont tendance à utiliser moins de mémoire et à offrir de meilleures performances en raison de la génération du code au moment de la compilation. Pour éliminer les démarrages à froid des fonctions, envisagez de passer à la sérialisation générée par la source.

> **Note**
>
> Si vous souhaitez utiliser la compilation native anticipée (AOT) avec Lambda, vous devez utiliser la sérialisation générée à la source.

File-based fonctions

Introduites dans .NET 10, les applications basées sur des fichiers vous permettent de créer des applications .NET à partir d'un seul `.cs` fichier, sans structure de `.csproj` fichier ou de répertoire. Lambda prend en charge les fonctions basées sur des fichiers, à commencer par .NET 10. Ils offrent un moyen simple et léger de créer des fonctions d'événement Lambda en C#.

Le moyen le plus rapide de commencer à créer une fonction Lambda basée sur un fichier C# consiste à utiliser le package. `Amazon.Lambda.Templates` Pour installer le paquet, exécutez la commande suivante :

```
dotnet new install Amazon.Lambda.Templates
```

Ensuite, créez un exemple de fonction Lambda basée sur un fichier C# :

```
dotnet new lambda.FileBased -n MyLambdaFunction
```

File-based les fonctions utilisent des gestionnaires d'assemblages exécutables. Vous devez donc inclure le `Amazon.Lambda.RuntimeSupport` NuGet package et utiliser la `LambdaBootstrapBuilder.Create` méthode pour enregistrer la fonction de gestionnaire .NET pour le type d'événement et démarrer le client d'exécution .NET Lambda.

File-based les fonctions utilisent .NET Native AOT par défaut, ce qui nécessite une sérialisation générée par la source. Vous pouvez désactiver l'AOT natif en le spécifiant `#:property PublishAot=false` dans votre fichier source. Pour plus d'informations sur l'utilisation de l'AOT natif dans Lambda, consultez. the section called “Compilation anticipée native”

Accès et utilisation de l’objet de contexte Lambda

L’objet de contexte Lambda contient des informations sur l’invocation, la fonction et l’environnement d’exécution. Dans cet exemple, l’objet de contexte est de type `Amazon.Lambda.Core.ILambdaContext`, et constitue le deuxième argument de la fonction de gestion principale.

```
public async Task<string> HandleRequest(Order order, ILambdaContext context) {
    ...
}
```

L’objet de contexte est une entrée facultative. Pour plus d’informations sur les signatures de gestionnaire acceptées valides, consultez the section called “Signatures de gestionnaire valides pour les fonctions C#”.

L'objet de contexte est utile pour générer des journaux de fonctions pour Amazon CloudWatch. Vous pouvez utiliser la méthode `context.getLogger()` pour obtenir un objet `LambdaLogger` pour l’enregistrement. Dans cet exemple, nous pouvons utiliser l’enregistreur pour enregistrer un message d’erreur si le traitement échoue pour une raison quelconque :

```
context.Logger.LogError($"Failed to process order: {ex.Message}");
```

En dehors de la journalisation, vous pouvez également utiliser l’objet de contexte pour surveiller les fonctions. Pour plus d’informations sur la copie d’objets, consultez the section called “Contexte”.

Utilisation de SDK pour .NET v3 dans votre gestionnaire

Vous utiliserez souvent les fonctions Lambda pour interagir avec d'autres AWS ressources ou pour les mettre à jour. Le moyen le plus simple d'interagir avec ces ressources est d'utiliser la SDK pour .NET version 3.

> **Note**
>
> Le SDK pour .NET (v2) est obsolète. Nous vous recommandons de n'utiliser que la SDK pour .NET version 3.

Vous pouvez ajouter des dépendances du SDK à votre projet à l'aide de la commande `Amazon.Lambda.Tools` suivante :

```
dotnet add package <package_name>
```

Par exemple, dans l'exemple principal sur cette page, nous devons utiliser l'API Amazon S3 pour charger un reçu sur S3. Nous pouvons importer le client du SDK Amazon S3 à l'aide de la commande suivante :

```
dotnet add package AWSSDK.S3
```

Cette commande ajoute la dépendance à votre projet. Vous devriez également voir une ligne similaire à la suivante dans le fichier `.csproj` de votre projet :

```
<PackageReference Include="AWSSDK.S3" Version="3.7.2.18" />
```

Importez ensuite les dépendances directement dans votre code C# :

```
using Amazon.S3;
using Amazon.S3.Model;
```

L'exemple de code initialise ensuite un client Amazon S3 (en utilisant la chaîne de fournisseur d'informations d'identification par défaut) comme suit :

```
private static readonly AmazonS3Client s3Client = new();
```

Dans cet exemple, nous avons initialisé notre client Amazon S3 en dehors de la fonction de gestionnaire principale pour éviter d'avoir à l'initialiser à chaque fois que nous invoquons notre fonction. Après avoir initialisé votre client SDK, vous pouvez l'utiliser pour interagir avec d'autres AWS services. L'exemple de code appelle l'API Amazon S3 `PutObject` comme suit :

```
var putRequest = new PutObjectRequest
```

```
{
    BucketName = bucketName,
    Key = key,
    ContentBody = receiptContent,
    ContentType = "text/plain"
};

await s3Client.PutObjectAsync(putRequest);
```

Accès aux variables d'environnement

Dans le code de votre gestionnaire, vous pouvez référencer n'importe quelle variable d'environnement à l'aide de la méthode `System.Environment.GetEnvironmentVariable`. Dans cet exemple, nous référençons la variable d'environnement `RECEIPT_BUCKET` définie à l'aide des lignes de code suivantes :

```
string? bucketName = Environment.GetEnvironmentVariable("RECEIPT_BUCKET");
if (string.IsNullOrWhiteSpace(bucketName))
{
    throw new ArgumentException("RECEIPT_BUCKET environment variable is not set");
}
```

Utilisation de l'état global

Lambda exécute votre code statique et le constructeur de classe pendant la phase d'initialisation avant d'invoquer votre fonction pour la première fois. Les ressources créées pendant l'initialisation restent en mémoire entre les invocations, ce qui vous évite d'avoir à les créer chaque fois que vous invoquez votre fonction.

Dans l'exemple de code, le code d'initialisation du client S3 se trouve en dehors de la méthode du gestionnaire principal. L'exécution initialise le client avant que la fonction exécute son premier événement, ce qui peut entraîner des délais de traitement plus longs. Les événements suivants sont beaucoup plus rapides, car Lambda n'a pas besoin d'initialiser à nouveau le client.

Simplifiez le code de la fonction à l'aide du cadre d'annotations Lambda

Les annotations Lambda constituent un cadre pour .NET 8 qui simplifie l'écriture des fonctions Lambda en utilisant C#. Le cadre d'annotations utilise des générateurs de source pour générer un code qui traduit le modèle de programmation Lambda en code simplifié. Grâce au cadre d'annotations, vous pouvez remplacer une grande partie du code d'une fonction Lambda écrite à

l'aide du modèle de programmation habituel. Le code écrit à l'aide du cadre utilise des expressions plus simples qui vous permettent de vous concentrer sur votre logique commerciale. Consultez Amazon.Lambda.Annotationsla documentation de Nuget pour des exemples.

Pour un exemple d'application complète utilisant les annotations Lambda, consultez l' PhotoAssetManagerexemple dans le référentiel. `awsdocs/aws-doc-sdk-examples` GitHub Le fichier `Function.cs` principal dans le répertoire `PamApiAnnotations` utilise des annotations Lambda. À titre de comparaison, le répertoire `PamApi` contient des fichiers équivalents écrits à l'aide du modèle de programmation Lambda habituel.

Injection de dépendances grâce au cadre d'annotations Lambda

Vous pouvez également utiliser le cadre d'annotations Lambda pour ajouter l'injection de dépendance à vos fonctions Lambda en utilisant une syntaxe que vous connaissez bien. Lorsque vous ajoutez un `[LambdaStartup]` attribut à un `Startup.cs` fichier, le framework Lambda Annotations génère le code requis au moment de la compilation.

```
[LambdaStartup]
public class Startup
{
    public void ConfigureServices(IServiceCollection services)
    {
        services.AddSingleton<IDatabaseRepository, DatabaseRepository>();
    }
}
```

Votre fonction Lambda peut injecter des services en utilisant l'injection de constructeur ou en injectant dans des méthodes individuelles à l'aide de l'attribut `[FromServices]`.

```
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSerializer

namespace GetProductHandler;

public class Function
{
    private readonly IDatabaseRepository _repo;

    public Function(IDatabaseRepository repo)
    {
```

```
        this._repo = repo;
    }

    [LambdaFunction]
    [HttpApi(LambdaHttpMethod.Get, "/product/{id}")]
    public async Task<Product> FunctionHandler([FromServices] IDatabaseRepository
 repository, string id)
    {
        return await this._repo.GetById(id);
    }
}
```

Meilleures pratiques en matière de code pour les fonctions d'événement Lambda en C#

Respectez les directives de la liste suivante pour utiliser les pratiques exemplaires de codage lors de la création de vos fonctions Lambda :

- Séparez le gestionnaire Lambda de votre logique principale. Avec cette approche, vous pouvez créer une fonction plus testable à l'unité.
- Contrôlez les dépendances du package de déploiement de vos fonctions. L'environnement d'exécution AWS Lambda contient un certain nombre de bibliothèques. Pour activer les dernières fonctionnalités et mises à jour de sécurité, Lambda met régulièrement à jour ces bibliothèques. Ces mises à jour peuvent apporter des modifications subtiles au comportement de votre fonction Lambda. Pour disposer du contrôle total des dépendances que votre fonction utilise, empaquetez toutes vos dépendances avec votre package de déploiement.
- Réduisez la complexité de vos dépendances. Privilégiez les infrastructures plus simples qui se chargent rapidement au démarrage de l'environnement d'exécution.
- Réduisez la taille de votre package de déploiement selon ses besoins d'exécution. Cela réduit le temps nécessaire au téléchargement et au déballage de votre package de déploiement avant l'invocation. Pour les fonctions créées dans .NET, évitez de télécharger l'intégralité de la bibliothèque du AWS SDK dans le cadre de votre package de déploiement. Dépendez plutôt de manière sélective des modules qui récupèrent les composants du SDK dont vous avez besoin (par exemple, DynamoDB, les modules du SDK Amazon S3 et les bibliothèques principales Lambda).

Tirez parti de la réutilisation de l'environnement d'exécution pour améliorer les performances de votre fonction. Initialisez les clients SDK et les connexions à la base de données en dehors du gestionnaire de fonctions et mettez en cache les actifs statiques localement dans le répertoire `/tmp`. Les invocations ultérieures traitées par la même instance de votre fonction peuvent réutiliser

ces ressources. Cela permet d'économiser des coûts, tout en réduisant le temps d'exécution de la fonction.

Pour éviter des éventuelles fuites de données entre les invocations, n'utilisez pas l'environnement d'exécution pour stocker des données utilisateur, des événements ou d'autres informations ayant un impact sur la sécurité. Si votre fonction repose sur un état réversible qui ne peut pas être stocké en mémoire dans le gestionnaire, envisagez de créer une fonction distincte ou des versions distinctes d'une fonction pour chaque utilisateur.

Utilisez une directive keep-alive pour maintenir les connexions persistantes. Lambda purge les connexions inactives au fil du temps. Si vous tentez de réutiliser une connexion inactive lorsque vous invoquez une fonction, cela entraîne une erreur de connexion. Pour maintenir votre connexion persistante, utilisez la directive Keep-alive associée à votre environnement d'exécution. Pour un exemple, voir Réutilisation des connexions avec Keep-Alive in Node.js.

Utilisez des variables d'environnement pour transmettre des paramètres opérationnels à votre fonction. Par exemple, si vous écrivez dans un compartiment Amazon S3 au lieu de coder en dur le nom du compartiment dans lequel vous écrivez, configurez le nom du compartiment comme variable d'environnement.

Évitez d'utiliser des invocations récursives dans votre fonction Lambda, lorsque la fonction s'invoque elle-même ou démarre un processus susceptible de l'invoquer à nouveau. Cela peut entraîner un volume involontaire d'invocations de fonction et des coûts accrus. Si vous constatez un volume involontaire d'invocations, définissez immédiatement la simultanéité réservée à la fonction sur `0` afin de limiter toutes les invocations de la fonction, pendant que vous mettez à jour le code.

N'utilisez pas d'API non publiques non documentées dans le code de votre fonction Lambda. Pour les AWS Lambda environnements d'exécution gérés, Lambda applique régulièrement des mises à jour fonctionnelles et de sécurité aux API internes de Lambda. Ces mises à jour internes de l'API peuvent être incompatibles avec les versions antérieures, entraînant des conséquences imprévues telles que des échecs d'invocation si votre fonction dépend de ces API non publiques. Consultez la Référence d'API pour obtenir la liste des API accessibles au public.

Écriture du code idempotent. L'écriture de code idempotent pour vos fonctions garantit ne gestion identique des événements dupliqués. Votre code doit valider correctement les événements et gérer correctement les événements dupliqués. Pour de plus amples informations, veuillez consulterComment faire en sorte que ma fonction Lambda soit idempotente ?.

Créez et déployez des fonctions d'événement Lambda C# avec des archives de fichiers .zip

Un package de déploiement .NET (archive de fichier .zip) contient l'assemblage compilé de votre fonction ainsi que toutes les dépendances de l'assemblage. Le package contient également un fichier *proj*`.deps.json`. Il indique à l'exécution .NET toutes les dépendances de votre fonction et un fichier *proj*`.runtimeconfig.json`, qui est utilisé pour configurer l'exécution.

Pour déployer des fonctions d'événement Lambda individuelles, vous pouvez utiliser la CLI globale .NET `Amazon.Lambda.Tools` Lambda. L'utilisation de la commande `dotnet lambda deploy-function` crée automatiquement un package de déploiement .zip et le déploie sur Lambda. Toutefois, nous vous recommandons d'utiliser des frameworks tels que le AWS Serverless Application Model (AWS SAM) ou le Cloud Development Kit AWS (AWS CDK) pour déployer vos applications .NET AWS.

Les applications sans serveur comprennent généralement une combinaison de fonctions Lambda et d'autres fonctions Services AWS gérées qui fonctionnent ensemble pour effectuer une tâche métier particulière. AWS SAM et AWS CDK simplifiez la création et le déploiement de fonctions Lambda avec d'autres fonctions Services AWS à grande échelle. La spécification du AWS SAM modèle fournit une syntaxe simple et claire pour décrire les fonctions Lambda, les API, les autorisations, les configurations et les autres AWS ressources qui constituent votre application sans serveur. Grâce au AWS CDK, vous pouvez définir l'infrastructure cloud en tant que code pour vous aider à créer des applications fiables, évolutives et rentables dans le cloud à l'aide de langages de programmation et de cadres modernes tels que .NET. Vous pouvez AWS SAM utiliser AWS CDK la CLI globale .NET Lambda pour empaqueter vos fonctions.

Bien qu'il soit possible d'utiliser des couches Lambda avec des fonctions en C# à l'aide de la CLI .NET Core, nous vous le déconseillons. Les fonctions en C# qui utilisent des couches chargent manuellement les assemblages partagés dans la mémoire pendant le Phase d'initialisation, ce qui peut augmenter les temps de démarrage à froid. Incluez plutôt tout le code partagé au moment de la compilation pour éviter d'affecter les performances du chargement des assemblages au moment de l'exécution.

Vous trouverez des instructions pour créer et déployer des fonctions .NET Lambda à l'aide de la AWS SAM CLI globale .NET Lambda et du .NET Lambda dans les sections suivantes. AWS CDK

Rubriques

- Utilisation de la CLI .NET Lambda Global

- Déployez les fonctions d'événement Lambda C# à l'aide de AWS SAM
- Déployez les fonctions d'événement Lambda C# à l'aide de AWS CDK
- Déployer ASP.NET des applications

Utilisation de la CLI .NET Lambda Global

La CLI .NET et l'extension .NET Lambda Global Tools (`Amazon.Lambda.Tools`) offrent une méthode de création multiplateforme. NET-based Applications Lambda, empaquetez-les et déployez-les sur Lambda. Dans cette section, vous apprendrez à créer de nouveaux projets Lambda .NET à l'aide de la CLI .NET et des modèles Amazon Lambda, et à les empaqueter et les déployer en utilisant `Amazon.Lambda.Tools`

Rubriques

- Conditions préalables
- Création de projets .NET à l'aide de la CLI .NET
- Déploiement de projets .NET à l'aide de la CLI .NET
- Utilisation de couches Lambda avec l'interface de ligne de commande .NET

Conditions préalables

Kit SDK .NET 8

Si vous ne l'avez pas encore fait, installez le kit SDK .NET 8 et l'environnement d'exécution.

AWS Amazon.Lambda.Templates Modèles de projets .NET

Pour générer le code de votre fonction Lambda, utilisez le Amazon.Lambda.Templates NuGet package. Pour installer ce package de modèle, exécutez la commande suivante :

```
dotnet new install Amazon.Lambda.Templates
```

AWS Amazon.Lambda.Tools Outils .NET Global CLI

Pour créer vos fonctions Lambda, utilisez l'Amazon.Lambda.Tools extension outils globaux .NET. Pour installer Amazon.Lambda.Tools, exécutez la commande suivante :

```
dotnet tool install -g Amazon.Lambda.Tools
```

Pour plus d'informations sur l'extension Amazon.Lambda.Tools .NET CLI, consultez le référentiel AWS Extensions for .NET CLI sur GitHub.

Création de projets .NET à l'aide de la CLI .NET

Dans la CLI .NET, utilisez la commande `dotnet new` pour créer des projets .NET à partir de la ligne de commande. Lambda propose des modèles supplémentaires à l'aide du Amazon.Lambda.Templates NuGet package.

Après avoir installé ce package, exécutez la commande suivante pour obtenir la liste des modèles disponibles.

```
dotnet new list
```

Pour examiner les détails relatifs à un modèle, utilisez l'option `help`. Par exemple, pour obtenir des détails sur le modèle `lambda.EmptyFunction`, exécutez la commande suivante.

```
dotnet new lambda.EmptyFunction --help
```

Pour créer un modèle de base pour une fonction Lambda .NET, utilisez le modèle `lambda.EmptyFunction`. Celui-ci crée une fonction simple qui prend une chaîne comme entrée et la convertit en majuscules à l'aide de la méthode `ToUpper`. Ce modèle prend en charge les options suivantes :

- `--name` – Nom de la fonction.
- `--region`— La AWS région dans laquelle créer la fonction.
- `--profile`— Le nom d'un profil dans votre fichier AWS SDK pour .NET d'informations d'identification. Pour en savoir plus sur les profils d'identification dans .NET, consultez la section Configurer les AWS informations d'identification dans le Guide du développeur du AWS SDK for .NET.

Dans cet exemple, nous créons une nouvelle fonction vide nommée `myDotnetFunction` en utilisant le profil et les Région AWS paramètres par défaut :

```
dotnet new lambda.EmptyFunction --name myDotnetFunction
```

Cette commande crée les fichiers et répertoires suivants dans le répertoire de votre projet.

```
### myDotnetFunction
    ### src
    #   ### myDotnetFunction
    #       ### Function.cs
    #       ### Readme.md
    #       ### aws-lambda-tools-defaults.json
    #       ### myDotnetFunction.csproj
    ### test
        ### myDotnetFunction.Tests
            ### FunctionTest.cs
            ### myDotnetFunction.Tests.csproj
```

Sous le répertoire `src/myDotnetFunction`, examinez les fichiers suivants :

- aws-lambda-tools-defaults.json : c'est ici que vous spécifiez les options de ligne de commande lors du déploiement de votre fonction Lambda. Par exemple :

  ```
    "profile" : "default",
    "region" : "us-east-2",
    "configuration" : "Release",
    "function-architecture": "x86_64",
    "function-runtime":"dotnet8",
    "function-memory-size" : 256,
    "function-timeout" : 30,
    "function-handler" : "myDotnetFunction::myDotnetFunction.Function::FunctionHandler"
  ```

- Function.cs: le code de fonction de votre gestionnaire Lambda. Il s'agit d'un modèle C # qui inclut la bibliothèque `Amazon.Lambda.Core` par défaut et un attribut `LambdaSerializer` par défaut. Pour plus d'informations sur les conditions de sérialisation et les options, consultez Sérialisation dans les fonctions d'événement Lambda en C#. Il inclut également un exemple de fonction que vous pouvez modifier pour appliquer votre code de fonction Lambda.

  ```
  using Amazon.Lambda.Core;

  // Assembly attribute to enable the Lambda function's JSON input to be converted into
   a .NET class.
  [assembly:
   LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSerializ

  namespace myDotnetFunction;
  ```

```
public class Function
{

    /// <summary>
    /// A simple function that takes a string and does a ToUpper
    /// </summary#
    /// <param name="input"></param>
    /// <param name="context"></param>
    /// <returns></returns>
    public string FunctionHandler(string input, ILambdaContext context)
    {
        return input.ToUpper();
    }
}
```

- my DotnetFunction.csproj : fichier MSBuild qui répertorie les fichiers et les assemblages qui composent votre application.

```
<Project Sdk="Microsoft.NET.Sdk">
  <PropertyGroup>
    <TargetFramework>net8.0</TargetFramework>
    <ImplicitUsings>enable</ImplicitUsings>
    <Nullable>enable</Nullable>
    <GenerateRuntimeConfigurationFiles>true</GenerateRuntimeConfigurationFiles>
    <AWSProjectType>Lambda</AWSProjectType>
    <!-- This property makes the build directory similar to a publish directory and
 helps the AWS .NET Lambda Mock Test Tool find project dependencies. -->
    <CopyLocalLockFileAssemblies>true</CopyLocalLockFileAssemblies>
    <!-- Generate ready to run images during publishing to improve cold start time.
 -->
    <PublishReadyToRun>true</PublishReadyToRun>
  </PropertyGroup>
  <ItemGroup>
    <PackageReference Include="Amazon.Lambda.Core" Version="2.2.0" />
    <PackageReference Include="Amazon.Lambda.Serialization.SystemTextJson"
 Version="2.4.0" />
  </ItemGroup>
</Project>
```

- Readme : utilisez ce fichier pour documenter votre fonction Lambda.

Sous le répertoire `myfunction/test`, examinez les fichiers suivants :

- my DotnetFunction.Tests.csproj : Comme indiqué précédemment, il s'agit d'un fichier MSBuild qui répertorie les fichiers et les assemblages qui composent votre projet de test. Notez également qu'il comprend aussi la bibliothèque `Amazon.Lambda.Core`, ce qui vous permet d'intégrer de manière transparente tout modèle Lambda requis pour tester votre fonction.

```
<Project Sdk="Microsoft.NET.Sdk">
   ...

    <PackageReference Include="Amazon.Lambda.Core" Version="2.2.0 " />
   ...
```

- FunctionTest.cs: le même fichier de modèle de code C# que celui inclus dans le `src` répertoire. Modifiez ce fichier pour mettre en miroir le code de production de votre fonction, et testez-le avant de télécharger votre fonction Lambda sur un environnement de production.

```
using Xunit;
using Amazon.Lambda.Core;
using Amazon.Lambda.TestUtilities;

using MyFunction;

namespace MyFunction.Tests
{
    public class FunctionTest
    {
        [Fact]
        public void TestToUpperFunction()
        {

            // Invoke the lambda function and confirm the string was upper cased.
            var function = new Function();
            var context = new TestLambdaContext();
            var upperCase = function.FunctionHandler("hello world", context);

            Assert.Equal("HELLO WORLD", upperCase);
        }
    }
}
```

Déploiement de projets .NET à l'aide de la CLI .NET

Pour créer votre package de déploiement et le déployer sur Lambda, utilisez les outils CLI `Amazon.Lambda.Tools`. Pour déployer votre fonction à partir des fichiers que vous avez créés dans les étapes précédentes, accédez d'abord au dossier contenant le fichier `.csproj` de votre fonction.

```
cd myDotnetFunction/src/myDotnetFunction
```

Pour déployer votre code sur Lambda sous la forme d'un package de déploiement .zip, exécutez la commande suivante. Choisissez le nom de votre fonction.

```
dotnet lambda deploy-function myDotnetFunction
```

Pendant le déploiement, l'assistant vous invite à sélectionner un the section called "Rôle d'exécution (autorisations pour les fonctions d'accéder à d'autres ressources)". Pour cet exemple, sélectionnez le `lambda_basic_role`.

Une fois votre fonction déployée, vous pouvez la tester dans le cloud en utilisant la commande `dotnet lambda invoke-function`. Pour l'exemple de code dans le modèle `lambda.EmptyFunction`, vous pouvez tester votre fonction en transmettant une chaîne en utilisant l'option `--payload`.

```
dotnet lambda invoke-function myDotnetFunction --payload "Just checking if everything
 is OK"
```

Si votre fonction a été déployée avec succès, vous devriez obtenir une sortie similaire à celle qui suit.

```
dotnet lambda invoke-function myDotnetFunction --payload "Just checking if everything
 is OK"
Amazon Lambda Tools for .NET Core applications (5.8.0)
Project Home: https://github.com/aws/aws-extensions-for-dotnet-cli, https://github.com/
aws/aws-lambda-dotnet

Payload:
"JUST CHECKING IF EVERYTHING IS OK"

Log Tail:
START RequestId: id Version: $LATEST
```

```
END RequestId: id
REPORT RequestId: id  Duration: 0.99 ms       Billed Duration: 1 ms         Memory
 Size: 256 MB     Max Memory Used: 12 MB
```

Utilisation de couches Lambda avec l'interface de ligne de commande .NET

> **Note**
>
> Bien qu'il soit possible d'utiliser des couches avec dans .NET, nous vous le déconseillons. Les fonctions en .NET qui utilisent des couches chargent manuellement les assemblages partagés dans la mémoire pendant la phase `Init`, ce qui peut augmenter les temps de démarrage à froid. Incluez plutôt tout le code partagé au moment de la compilation pour tirer parti des optimisations intégrées du compilateur .NET.

L'interface de ligne de commande .NET prend en charge les commandes qui vous aident à publier des couches et à déployer des fonctions C# consommant des couches. Pour publier une couche dans un compartiment Amazon S3 spécifié, exécutez la commande suivante dans le même répertoire que votre fichier `.csproj` :

```
dotnet lambda publish-layer <layer_name> --layer-type runtime-package-store --s3-
bucket <s3_bucket_name>
```

Ensuite, lorsque vous déployez votre fonction à l'aide de l'interface de ligne de commande .NET, spécifiez l'ARN de couche à consommer dans la commande suivante :

```
dotnet lambda deploy-function <function_name> --function-layers arn:aws:lambda:us-
east-1:123456789012:layer:layer-name:1
```

Pour un exemple complet de fonction Hello World, consultez l'exemple blank-csharp-with-layer.

Déployez les fonctions d'événement Lambda C# à l'aide de AWS SAM

The AWS Serverless Application Model (AWS SAM) est une boîte à outils qui permet de rationaliser le processus de création et d'exécution d'applications sans serveur sur AWS. Vous définissez les ressources de votre application dans un modèle YAML ou JSON et vous utilisez l'interface de ligne de AWS SAM commande (AWS SAM CLI) pour créer, empaqueter et déployer vos applications. Lorsque vous créez une fonction Lambda à partir d'un AWS SAM modèle, elle crée AWS SAM

automatiquement un package de déploiement ou une image de conteneur .zip avec le code de votre fonction et les dépendances que vous spécifiez. AWS SAM déploie ensuite votre fonction à l'aide d'une CloudFormation pile. Pour en savoir plus sur l'utilisation des fonctions Lambda AWS SAM pour créer et déployer des fonctions Lambda, consultez la section Getting started with AWS SAM dans le Guide du AWS Serverless Application Model développeur.

Les étapes suivantes vous montrent comment télécharger, créer et déployer un exemple d'application Hello World en .NET à l'aide de AWS SAM. Cet exemple d'application utilise une fonction Lambda et un point de terminaison Amazon API Gateway pour implémenter une API backend de base. Lorsque vous envoyez une requête HTTP GET à votre point de terminaison API Gateway, API Gateway invoque votre fonction Lambda. La fonction renvoie un message « hello world », ainsi que l'adresse IP de l'instance de la fonction Lambda qui traite votre requête.

Lorsque vous créez et déployez votre application en utilisant AWS SAM, en arrière-plan, la AWS SAM CLI utilise la `dotnet lambda package` commande pour empaqueter les ensembles de codes de fonction Lambda individuels.

Conditions préalables

Kit SDK .NET 8

Installez l'environnement d'exécution et le kit SDK .NET 8.

AWS SAM CLI version 1.39 ou ultérieure

Pour savoir comment installer la dernière version de la AWS SAM CLI, reportez-vous à la section Installation de la AWS SAM CLI.

Déployer un échantillon AWS SAM vigie

1. Initialisez l'application en utilisant le modèle Hello world .NET à l'aide de la commande suivante.

```
sam init --app-template hello-world --name sam-app \
--package-type Zip --runtime dotnet8
```

Cette commande crée les fichiers et répertoires suivants dans le répertoire de votre projet.

```
### sam-app
    ### README.md
    ### events
    #   ### event.json
```

```
    ### omnisharp.json
    ### samconfig.toml
    ### src
    #   ### HelloWorld
    #       ### Function.cs
    #       ### HelloWorld.csproj
    #       ### aws-lambda-tools-defaults.json
    ### template.yaml
    ### test
        ### HelloWorld.Test
            ### FunctionTest.cs
            ### HelloWorld.Tests.csproj
```

2. Accédez au répertoire contenant le `template.yaml file`. Ce fichier est un modèle qui définit les ressources AWS de votre application, notamment votre fonction Lambda et API Gateway.

```
cd sam-app
```

3. Pour créer la source de votre application, exécutez la commande suivante.

```
sam build
```

4. Pour déployer votre application sur AWS, exécutez la commande suivante.

```
sam deploy --guided
```

Cette commande permet d'empaqueter et de déployer votre application à l'aide de la série d'invites suivante. Pour accepter les options par défaut, appuyez sur Entrée.

> **Note**
>
> Car l'autorisation n'a HelloWorldFunction peut-être pas été définie, est-ce que ça va ? , assurez-vous d'entrery.

- Nom de la pile : nom de la pile à déployer sur CloudFormation. Ce nom doit être propre à votre Compte AWS et Région AWS.
- Région AWS: le sur lequel Région AWS vous souhaitez déployer votre application.
- Confirmer les modifications avant le déploiement : sélectionnez oui pour examiner manuellement tous les ensembles de modifications avant que AWS SAM ne déploie

les modifications de l'application. Si vous sélectionnez Non, la AWS SAM CLI déploie automatiquement les modifications apportées aux applications.

- Autoriser la création de rôles IAM dans la CLI SAM : de nombreux AWS SAM modèles, y compris celui de Hello world dans cet exemple, créent des rôles Gestion des identités et des accès AWS (IAM) pour autoriser vos fonctions Lambda à accéder à d'autres. Services AWS Sélectionnez Oui pour autoriser le déploiement d'une CloudFormation pile qui crée ou modifie des rôles IAM.
- Désactiver le rollback : par défaut, AWS SAM en cas d'erreur lors de la création ou du déploiement de votre stack, il rétablit la version précédente. Sélectionnez Non pour accepter cette valeur par défaut.
- HelloWorldFunction l'autorisation n'est peut-être pas définie, est-ce que ça va : Entrezy.
- Enregistrer les arguments dans samconfig.toml : sélectionnez oui pour enregistrer vos choix de configuration. À l'avenir, vous pourrez à nouveau exécuter `sam deploy` sans paramètres pour déployer les modifications apportées à votre application.

5. Une fois le déploiement de votre application terminé, la CLI renvoie l'Amazon Resource Name (ARN) de la fonction Lambda Hello World et le rôle IAM créé pour cette fonction. Elle affiche également le point de terminaison de votre API Gateway. Pour tester votre application, ouvrez le point de terminaison dans un navigateur. Vous devriez voir une réponse similaire à la suivante.

```
{"message":"hello world","location":"34.244.135.203"}
```

6. Pour supprimer vos ressources, exécutez la commande suivante. Notez que le point de terminaison de l'API que vous avez créé est un point de terminaison public accessible via le réseau Internet. Nous vous recommandons de supprimer ce point de terminaison après les tests.

```
sam delete
```

Étapes suivantes

Pour en savoir plus sur la création et le déploiement de fonctions Lambda AWS SAM à l'aide de .NET, consultez les ressources suivantes :

- Le AWS Serverless Application Model Guide du développeur (AWS SAM)
- Création d'applications .NET sans serveur à l'aide de AWS Lambda la CLI SAM

Déployez les fonctions d'événement Lambda C# à l'aide de AWS CDK

Cloud Development Kit AWS (AWS CDK) Il s'agit d'un framework de développement logiciel open source permettant de définir l'infrastructure cloud comme du code avec des langages de programmation modernes et des frameworks tels que .NET. AWS CDK les projets sont exécutés pour générer des CloudFormation modèles qui sont ensuite utilisés pour déployer votre code.

Pour créer et déployer un exemple d'application Hello world .NET à l'aide de AWS CDK, suivez les instructions des sections suivantes. L'exemple d'application implémente une API backend de base composée d'un point de terminaison API Gateway et d'une fonction Lambda. Lorsque vous envoyez une requête HTTP GET au point de terminaison, API Gateway invoque la fonction Lambda. La fonction renvoie un message Hello world, ainsi que l'adresse IP de l'instance Lambda qui traite votre requête.

Conditions préalables

Kit SDK .NET 8

Installez l'environnement d'exécution et le kit SDK .NET 8.

AWS CDK version 2

Pour savoir comment installer la dernière version de la version 2, AWS CDK voir Getting started with the AWS CDK in the Cloud Development Kit AWS (AWS CDK) v2 Developer Guide.

Déployer un échantillon AWS CDK vigie

1. Créez un répertoire de projet pour l'application modèle et accédez à ce répertoire.

```
mkdir hello-world
cd hello-world
```

2. Initialisez une nouvelle AWS CDK application en exécutant la commande suivante.

```
cdk init app --language csharp
```

La commande crée les fichiers et répertoires suivants dans votre répertoire de projet.

```
### README.md
### cdk.json
```

```
### src
    ### HelloWorld
    #   ### GlobalSuppressions.cs
    #   ### HelloWorld.csproj
    #   ### HelloWorldStack.cs
    #   ### Program.cs
    ### HelloWorld.sln
```

3. Ouvrez le répertoire `src` et créez une nouvelle fonction Lambda à l'aide de la CLI .NET. Il s'agit de la fonction que vous déployez à l'aide du AWS CDK. Dans cet exemple, vous créez une fonction Hello world nommée `HelloWorldLambda` à l'aide du modèle `lambda.EmptyFunction`.

```
cd src
dotnet new lambda.EmptyFunction -n HelloWorldLambda
```

Après cette étape, la structure de votre répertoire à l'intérieur de votre répertoire de projet devrait ressembler à ce qui suit.

```
### README.md
### cdk.json
### src
    ### HelloWorld
    #   ### GlobalSuppressions.cs
    #   ### HelloWorld.csproj
    #   ### HelloWorldStack.cs
    #   ### Program.cs
    ### HelloWorld.sln
    ### HelloWorldLambda
        ### src
        #   ### HelloWorldLambda
        #       ### Function.cs
        #       ### HelloWorldLambda.csproj
        #       ### Readme.md
        #       ### aws-lambda-tools-defaults.json
        ### test
            ### HelloWorldLambda.Tests
                ### FunctionTest.cs
                ### HelloWorldLambda.Tests.csproj
```

4. Ouvrez le fichier `HelloWorldStack.cs` à partir du répertoire `src/HelloWorld`. Remplacez le contenu du fichier par le code suivant.

```
using Amazon.CDK;
using Amazon.CDK.AWS.Lambda;
using Amazon.CDK.AWS.Logs;
using Constructs;

namespace CdkTest
{
    public class HelloWorldStack : Stack
    {
        internal HelloWorldStack(Construct scope, string id, IStackProps props =
 null) : base(scope, id, props)
        {
            var buildOption = new BundlingOptions()
            {
                Image = Runtime.DOTNET_8.BundlingImage,
                User = "root",
                OutputType = BundlingOutput.ARCHIVED,
                Command = new string[]{
            "/bin/sh",
                "-c",
                " dotnet tool install -g Amazon.Lambda.Tools"+
                " && dotnet build"+
                " && dotnet lambda package --output-package /asset-output/
function.zip"
                }
            };

             var helloWorldLambdaFunction = new Function(this,
 "HelloWorldFunction", new FunctionProps
            {
                Runtime = Runtime.DOTNET_8,
                MemorySize = 1024,
                LogRetention = RetentionDays.ONE_DAY,
                Handler =
 "HelloWorldLambda::HelloWorldLambda.Function::FunctionHandler",
                Code = Code.FromAsset("./src/HelloWorldLambda/src/
HelloWorldLambda", new Amazon.CDK.AWS.S3.Assets.AssetOptions
                {
                    Bundling = buildOption
                }),
            });
        }
    }
```

```
}
```

Il s'agit du code permettant de compiler et de regrouper le code de l'application, ainsi que de la définition de la fonction Lambda elle-même. L'objet `BundlingOptions` permet de créer un fichier zip, ainsi qu'un ensemble de commandes utilisées pour générer le contenu du fichier zip. Dans ce cas, la commande `dotnet lambda package` est utilisée pour compiler et générer le fichier zip.

5. Pour déployer votre application, exécutez la commande suivante.

```
cdk deploy
```

6. Invoquez votre fonction Lambda déployée à l'aide de la CLI .NET Lambda.

```
dotnet lambda invoke-function HelloWorldFunction -p "hello world"
```

7. Une fois les tests terminés, vous pouvez supprimer les ressources que vous avez créées, à moins que vous souhaitez les conserver. Exécutez la commande suivante pour supprimer vos ressources.

```
cdk destroy
```

Étapes suivantes

Pour en savoir plus sur la création et le déploiement de fonctions Lambda AWS CDK à l'aide de .NET, consultez les ressources suivantes :

- Travailler avec le AWS CDK en C#
- Créez, empaquetez et publiez des fonctions Lambda .NET C# avec le CDK AWS

Déployer ASP.NET des applications

En plus d'héberger des fonctions pilotées par des événements, vous pouvez également utiliser .NET avec Lambda Event Functions pour héberger des applications légères. ASP.NET Vous pouvez créer et déployer des ASP.NET applications à l'aide du `Amazon.Lambda.AspNetCoreServer` NuGet package. Dans cette section, vous apprendrez à déployer une API ASP.NET Web sur Lambda à l'aide de l'outil .NET Lambda CLI.

Rubriques

- Conditions préalables
- Déploiement d'une API ASP.NET Web sur Lambda
- Déploiement d' ASP.NET un minimum d'API sur Lambda

Conditions préalables

Kit SDK .NET 8

Installez le SDK .NET 8 et le ASP.NET Core Runtime.

Amazon.Lambda.Tools

Pour créer vos fonctions Lambda, utilisez l'Amazon.Lambda.Tools extension outils globaux .NET. Pour installer Amazon.Lambda.Tools, exécutez la commande suivante :

```
dotnet tool install -g Amazon.Lambda.Tools
```

Pour plus d'informations sur l'extension Amazon.Lambda.Tools .NET CLI, consultez le référentiel AWS Extensions for .NET CLI sur GitHub.

Amazon.Lambda.Templates

Pour générer le code de votre fonction Lambda, utilisez le Amazon.Lambda.Templates NuGet package. Pour installer ce package de modèle, exécutez la commande suivante :

```
dotnet new --install Amazon.Lambda.Templates
```

Déploiement d'une API ASP.NET Web sur Lambda

Pour déployer une API Web à l'aide des modèles .NET Lambda ASP.NET, vous pouvez utiliser les modèles .NET Lambda pour créer un nouveau projet d'API Web. Utilisez la commande suivante pour initialiser un nouveau projet d'API ASP.NET Web. Dans l'exemple de commande, nous nommons le projet `AspNetOnLambda`.

```
dotnet new serverless.AspNetCoreWebAPI -n AspNetOnLambda
```

Cette commande crée les fichiers et répertoires suivants dans le répertoire de votre projet.

```
.
### AspNetOnLambda
```

```
    ### src
    #   ### AspNetOnLambda
    #       ### AspNetOnLambda.csproj
    #       ### Controllers
    #       #   ### ValuesController.cs
    #       ### LambdaEntryPoint.cs
    #       ### LocalEntryPoint.cs
    #       ### Readme.md
    #       ### Startup.cs
    #       ### appsettings.Development.json
    #       ### appsettings.json
    #       ### aws-lambda-tools-defaults.json
    #       ### serverless.template
    ### test
        ### AspNetOnLambda.Tests
            ### AspNetOnLambda.Tests.csproj
            ### SampleRequests
            #   ### ValuesController-Get.json
            ### ValuesControllerTests.cs
            ### appsettings.json
```

Lorsque Lambda invoque votre fonction, le point d'entrée qu'elle utilise est le fichier `LambdaEntryPoint.cs`. Le fichier créé par le modèle Lambda .NET contient le code suivant.

```
namespace AspNetOnLambda;

public class LambdaEntryPoint : Amazon.Lambda.AspNetCoreServer.APIGatewayProxyFunction
{
    protected override void Init(IWebHostBuilder builder)
    {
        builder
            .UseStartup#Startup#();
    }

    protected override void Init(IHostBuilder builder)
    {
    }
}
```

Le point d'entrée utilisé par Lambda doit hériter de l'une des trois classes de base du package `Amazon.Lambda.AspNetCoreServer`. Ces trois classes de base sont les suivantes :

- `APIGatewayProxyFunction`

- `APIGatewayHttpApiV2ProxyFunction`
- `ApplicationLoadBalancerFunction`

La classe par défaut utilisée lorsque vous créez votre fichier `LambdaEntryPoint.cs` à l'aide du modèle Lambda .NET fourni est `APIGatewayProxyFunction`. La classe de base que vous utilisez dans votre fonction dépend de la couche d'API qui se trouve devant votre fonction Lambda.

Chacune des trois classes de base contient une méthode publique appelée `FunctionHandlerAsync`. Le nom de cette méthode fait partie de la chaîne du gestionnaire que Lambda utilise pour appeler votre fonction. Le `FunctionHandlerAsync` procédé transforme la charge utile des événements entrants dans le ASP.NET format correct et la ASP.NET réponse en retour à une charge utile de réponse Lambda. Pour l'exemple de projet `AspNetOnLambda` affiché, la chaîne du gestionnaire serait la suivante.

```
AspNetOnLambda::AspNetOnLambda.LambdaEntryPoint::FunctionHandlerAsync
```

Pour déployer l'API sur Lambda, exécutez les commandes suivantes pour accéder au répertoire contenant votre fichier de code source et déployer votre fonction à l'aide de CloudFormation.

```
cd AspNetOnLambda/src/AspNetOnLambda
dotnet lambda deploy-serverless
```

> **Tip**
>
> Lorsque vous déployez une API à l'aide de la **`dotnet lambda deploy-serverless`** commande, CloudFormation attribuez à votre fonction Lambda un nom basé sur le nom de pile que vous avez spécifié lors du déploiement. Pour donner un nom personnalisé à votre fonction Lambda, modifiez le fichier `serverless.template` pour ajouter une propriété `FunctionName` à la ressource `AWS::Serverless::Function`. Pour en savoir plus, consultez Type de nom dans le Guide de l'utilisateur CloudFormation .

Déploiement d' ASP.NET un minimum d'API sur Lambda

Pour déployer une API ASP.NET minimale sur Lambda, vous pouvez utiliser les modèles .NET Lambda pour créer un nouveau projet d'API minimale. Utilisez la commande suivante pour initialiser un nouveau projet d'API minimale. Dans cet exemple, nous nommons le projet `MinimalApiOnLambda`.

```
dotnet new serverless.AspNetCoreMinimalAPI -n MinimalApiOnLambda
```

La commande crée les fichiers et répertoires suivants dans le répertoire de votre projet.

```
### MinimalApiOnLambda
    ### src
        ### MinimalApiOnLambda
            ### Controllers
            #   ### CalculatorController.cs
            ### MinimalApiOnLambda.csproj
            ### Program.cs
            ### Readme.md
            ### appsettings.Development.json
            ### appsettings.json
            ### aws-lambda-tools-defaults.json
            ### serverless.template
```

Le fichier `Program.cs` contient le code suivant.

```
var builder = WebApplication.CreateBuilder(args);

// Add services to the container.
builder.Services.AddControllers();

// Add AWS Lambda support. When application is run in Lambda Kestrel is swapped out as
 the web server with Amazon.Lambda.AspNetCoreServer. This
// package will act as the webserver translating request and responses between the
 Lambda event source and ASP.NET Core.
builder.Services.AddAWSLambdaHosting(LambdaEventSource.RestApi);

var app = builder.Build();


app.UseHttpsRedirection();
app.UseAuthorization();
app.MapControllers();

app.MapGet("/", () => "Welcome to running ASP.NET Core Minimal API on AWS Lambda");

app.Run();
```

Pour configurer votre API minimale afin qu'elle s'exécute sur Lambda, vous devrez peut-être modifier ce code afin que les demandes et les réponses entre Lambda et ASP.NET Core soient correctement traduites. La fonction est configurée par défaut pour une source d'événements d'API REST. Pour une API HTTP ou un équilibreur de charge d'application, remplacez `(LambdaEventSource.RestApi)` par l'une des options suivantes :

- `(LambdaEventSource.HttpAPi)`
- `(LambdaEventSource.ApplicationLoadBalancer)`

Pour déployer votre API minimale sur Lambda, exécutez les commandes suivantes pour accéder au répertoire contenant votre fichier de code source et déployer votre fonction à l'aide de CloudFormation.

```
cd MinimalApiOnLambda/src/MinimalApiOnLambda
dotnet lambda deploy-serverless
```

Utilisation de couches pour les fonctions événementielles .NET Lambda

Nous déconseillons d'utiliser des couches pour gérer les dépendances des fonctions d'événement Lambda écrites en .NET. .NET étant un langage compilé, vos fonctions doivent toujours charger manuellement les assemblages partagés dans la mémoire pendant la phase d'initialisation, ce qui peut augmenter les temps de démarrage à froid. L'utilisation de couches complique non seulement le processus de déploiement, mais vous empêche également de tirer parti des optimisations du compilateur intégré.

Pour utiliser des dépendances externes avec vos gestionnaires .NET, incluez-les directement dans votre package de déploiement au moment de la compilation. Ce faisant, vous simplifiez le processus de déploiement et profitez des optimisations du compilateur .NET intégré. Pour un exemple d'importation et d'utilisation de dépendances telles que NuGet des packages dans votre fonction, consultezthe section called "Handler (Gestionnaire)".

Déployer les fonctions d'événement .NET Lambda avec des images de conteneur

Il existe trois méthodes pour créer une image de conteneur pour une fonction d'événement .NET Lambda :

- À l'aide d'un AWS image de base pour .NET

  Les images de base AWS sont préchargées avec une exécution du langage, un client d'interface d'exécution pour gérer l'interaction entre Lambda et votre code de fonction, et un émulateur d'interface d'exécution pour les tests locaux.
- À l'aide d'un AWS OS-only image de base

  AWS OS-only les images de base contiennent une distribution Amazon Linux et l'émulateur d'interface d'exécution. Ces images sont couramment utilisées pour créer des images de conteneur pour les langages compilés, tels que Go et Rust, et pour une langue ou une version linguistique pour laquelle Lambda ne fournit pas d'image de base, telle que Node.js 19. Vous pouvez également utiliser des images OS-only de base pour implémenter un environnement d'exécution personnalisé. Pour rendre l'image compatible avec Lambda, vous devez inclure le client d'interface d'exécution pour .NET dans l'image.
- Utilisation d'une image non AWS basique

  Vous pouvez utiliser une autre image de base à partir d'un autre registre de conteneur, comme Alpine Linux ou Debian. Vous pouvez également utiliser une image personnalisée créée par votre organisation. Pour rendre l'image compatible avec Lambda, vous devez inclure le client d'interface d'exécution pour .NET dans l'image.

> **Tip**
>
> Pour réduire le temps nécessaire à l'activation des fonctions du conteneur Lambda, consultez Utiliser des générations en plusieurs étapes (français non garanti) dans la documentation Docker. Pour créer des images de conteneur efficaces, suivez la section Bonnes pratiques pour l'écriture de Dockerfiles (français non garanti).

Cette page explique comment créer, tester et déployer des images de conteneur pour Lambda.

Rubriques

- AWS images de base pour .NET

- À l'aide d'un AWS image de base pour .NET
- Utilisation d’une autre image de base avec le client d’interface d’exécution

AWS images de base pour .NET

AWS fournit les images de base suivantes pour .NET :

Étiquettes	Environnement d’exécution	Système d’exploitation	Dockerfile	Obsolescence
10	.NET 10	Amazon Linux	Dockerfile pour .NET 10 sur GitHub	14 novembre 2028
9	.NET 9	Amazon Linux	Dockerfile pour .NET 9 sur GitHub	10 novembre 2026
8	.NET 8	Amazon Linux	Dockerfile pour .NET 8 sur GitHub	10 novembre 2026

Référentiel Amazon ECR : gallery.ecr. aws/lambda/point-net

À l'aide d'un AWS image de base pour .NET

Conditions préalables

Pour exécuter la procédure indiquée dans cette section, vous devez satisfaire aux exigences suivantes :

- SDK .NET : les étapes suivantes utilisent l’image de base .NET 8. Assurez-vous que votre version de .NET correspond à la version de l’image de base que vous spécifiez dans votre Dockerfile.
- Docker (version minimale 25.0.0)
- Le plug-in buildx Docker.

Création et déploiement d'une image à l'aide d'une image de base

Dans les étapes suivantes, vous allez utiliser Amazon.Lambda.Templateset Amazon.Lambda.Toolspour créer un projet .NET. Ensuite, vous créez une image Docker, vous chargez l'image sur Amazon ECR et vous la déployez vers une fonction Lambda.

1. Installez le package Amazon.Lambda.Templates NuGet .

```
dotnet new install Amazon.Lambda.Templates
```

2. Créez un projet .NET en utilisant le modèle `lambda.image.EmptyFunction`.

```
dotnet new lambda.image.EmptyFunction --name MyFunction --region us-east-1
```

   Les fichiers de projet sont stockés dans le répertoire *`MyFunction`*`/src/`*`MyFunction`* :

   - aws-lambda-tools-defaults.json : spécifie les options de ligne de commande pour le déploiement de votre fonction Lambda.
   - Function.cs: le code de fonction de votre gestionnaire Lambda. Il s'agit d'un modèle C# qui inclut la bibliothèque `Amazon.Lambda.Core` par défaut et un attribut `LambdaSerializer` par défaut. Pour plus d'informations sur les conditions de sérialisation et les options, consultez Sérialisation dans les fonctions d'événement Lambda en C#. Vous pouvez utiliser le code fourni pour les tests ou le remplacer par le vôtre.
   - MyFunction.csproj: fichier de projet .NET répertoriant les fichiers et les assemblages composant votre application.
   - Dockerfile : vous pouvez utiliser le Dockerfile fourni pour les tests ou le remplacer par le vôtre. Si vous utilisez le vôtre, assurez-vous de :
     - Définir la propriété `FROM` sur l'URI de l'image de base. L'image de base et `TargetFramework` dans le fichier `MyFunction.csproj` doivent tous deux utiliser la même version de .NET. Par exemple, pour utiliser .NET 9 :
       - Fichier Docker : `FROM` *`public.ecr.aws/lambda/dotnet:9`*
       - MyFunction.csproj: `<TargetFramework>`*`net9.0`*`</TargetFramework>`
     - Définir l'argument `CMD` pour le gestionnaire de la fonction Lambda. Il doit correspondre à `image-command` dans `aws-lambda-tools-defaults.json`.
3. Installez l'outil global Amazon.Lambda.Tools .NET.

```
dotnet tool install -g Amazon.Lambda.Tools
```

S' Amazon.Lambda.Tools il est déjà installé, assurez-vous de disposer de la dernière version.

```
dotnet tool update -g Amazon.Lambda.Tools
```

4. Changez le répertoire en *MyFunction*/src/*MyFunction*, si vous n'y êtes pas déjà.

```
cd src/MyFunction
```

5. Amazon.Lambda.Tools Utilisez-le pour créer l'image Docker, la transférer vers un nouveau référentiel Amazon ECR et déployer la fonction Lambda.

   Pour `--function-role`, indiquez le nom du rôle, et non l'Amazon Resource Name (ARN), du rôle d'exécution de la fonction. Par exemple : `lambda-role`.

```
dotnet lambda deploy-function MyFunction --function-role lambda-role
```

   Pour plus d'informations sur l'outil global Amazon.Lambda.Tools .NET, consultez le référentiel AWS Extensions for .NET CLI sur GitHub.

6. Invoquer la fonction.

```
dotnet lambda invoke-function MyFunction --payload "Testing the function"
```

   Si tout réussit, vous verrez une réponse similaire à ce qui suit :

```
Payload:
{"Lower":"testing the function","Upper":"TESTING THE FUNCTION"}

Log Tail:
INIT_REPORT Init Duration: 9999.81 ms   Phase: init     Status: timeout
START RequestId: 12378346-f302-419b-b1f2-deaa1e8423ed Version: $LATEST
END RequestId: 12378346-f302-419b-b1f2-deaa1e8423ed
REPORT RequestId: 12378346-f302-419b-b1f2-deaa1e8423ed  Duration: 3173.06 ms
 Billed Duration: 3174 ms        Memory Size: 512 MB     Max Memory Used: 24 MB
```

7. Supprimez la fonction Lambda.

```
dotnet lambda delete-function MyFunction
```

Utilisation d'une autre image de base avec le client d'interface d'exécution

Si vous utilisez une image OS-only de base ou une image de base alternative, vous devez inclure le client d'interface d'exécution dans votre image. Le client d'interface d'exécution étend leAPI de runtime, qui gère l'interaction entre Lambda et votre code de fonction.

L'exemple suivant montre comment créer une image de conteneur pour .NET à l'aide d'une image non AWS basique et comment ajouter le Amazon.Lambda.RuntimeSupport package, qui est le client d'interface d'exécution Lambda pour .NET. L'exemple de Dockerfile utilise l'image de base Microsoft .NET 8.

Conditions préalables

Pour exécuter la procédure indiquée dans cette section, vous devez satisfaire aux exigences suivantes :

- SDK .NET — Les étapes suivantes utilisent une image de base .NET 9. Assurez-vous que votre version de .NET correspond à la version de l'image de base que vous spécifiez dans votre Dockerfile.
- Docker (version minimale 25.0.0)
- Le plug-in buildx Docker.

Création et déploiement d'une image à l'aide d'une image de base alternative

1. Installez le package Amazon.Lambda.Templates NuGet .

   ```
   dotnet new install Amazon.Lambda.Templates
   ```

2. Créez un projet .NET en utilisant le modèle `lambda.CustomRuntimeFunction`. Ce modèle inclut le Amazon.Lambda.RuntimeSupportpackage.

   ```
   dotnet new lambda.CustomRuntimeFunction --name MyFunction --region us-east-1
   ```

3. Accédez au répertoire *MyFunction*`/src/`*MyFunction*. C'est ici que les fichiers du projet sont stockés. Examinez les fichiers suivants :

- aws-lambda-tools-defaults.json : c'est dans ce fichier que vous spécifiez les options de ligne de commande lors du déploiement de votre fonction Lambda.
- Function.cs— Le code contient une classe avec une `Main` méthode qui initialise la `Amazon.Lambda.RuntimeSupport` bibliothèque en tant que bootstrap. La méthode `Main` est le point d'entrée du processus de la fonction. La méthode `Main` enveloppe le gestionnaire de fonctions dans un encapsuleur avec lequel l'amorce peut travailler. Pour plus d'informations, voir Utilisation en Amazon.Lambda.RuntimeSupport tant que bibliothèque de classes dans le GitHub référentiel.
- MyFunction.csproj— Un fichier de projet .NET répertoriant les fichiers et les assemblages composant votre application.
- Readme.md— Ce fichier contient plus d'informations sur l'exemple de fonction Lambda.

4. Ouvrez le fichier `aws-lambda-tools-defaults.json` et ajoutez les lignes suivantes :

```
  "package-type": "image",
  "docker-host-build-output-dir": "./bin/Release/lambda-publish"
```

- package-typee : définit le package de déploiement en tant qu'image de conteneur.
- docker-host-build-output-dir : définit le répertoire de sortie pour le processus de génération.

Example aws-lambda-tools-defaults.json

```
{
  "Information": [
    "This file provides default values for the deployment wizard inside Visual
 Studio and the AWS Lambda commands added to the .NET Core CLI.",
    "To learn more about the Lambda commands with the .NET Core CLI execute the
 following command at the command line in the project root directory.",
    "dotnet lambda help",
    "All the command line options for the Lambda command can be specified in this
 file."
  ],
  "profile": "",
  "region": "us-east-1",
  "configuration": "Release",
  "function-runtime": "provided.al2023",
  "function-memory-size": 256,
  "function-timeout": 30,
```

```
  "function-handler": "bootstrap",
  "msbuild-parameters": "--self-contained true",
  "package-type": "image",
  "docker-host-build-output-dir": "./bin/Release/lambda-publish"
}
```

5. Créez un Dockerfile dans le référentiel *MyFunction*/src/*MyFunction*. L'exemple de Dockerfile suivant utilise une image de base Microsoft .NET au lieu d'une image de base AWS.

   - Définissez la propriété FROM pour l'identifiant de l'image de base. L'image de base et TargetFramework dans le fichier MyFunction.csproj doivent tous deux utiliser la même version de .NET.
   - Utilisez la commande COPY pour copier la fonction dans le répertoire /var/task.
   - Définissez le ENTRYPOINT sur le module que vous souhaitez que le conteneur Docker exécute lorsqu'il démarre. Dans ce cas, le module est l'amorce, qui initialise la bibliothèque Amazon.Lambda.RuntimeSupport.

   Notez que l'exemple de Dockerfile n'inclut pas d'instruction USER. Lorsque vous déployez une image de conteneur sur Lambda, Lambda définit automatiquement un utilisateur Linux par défaut disposant d'autorisations de moindre privilège. Ceci est différent du comportement standard de Docker qui est défini par défaut par l'utilisateur root lorsqu'aucune instruction USER n'est fournie.

   Example Dockerfile

```
# You can also pull these images from DockerHub amazon/aws-lambda-dotnet:8
FROM mcr.microsoft.com/dotnet/runtime:9.0

# Set the image's internal work directory
WORKDIR /var/task

# Copy function code to Lambda-defined environment variable
COPY "bin/Release/net9.0/linux-x64"  .

# Set the entrypoint to the bootstrap
ENTRYPOINT ["/usr/bin/dotnet", "exec", "/var/task/bootstrap.dll"]
```

6. Installez l'extension Amazon.Lambda.Tools .NET Global Tools.

```
dotnet tool install -g Amazon.Lambda.Tools
```

S' Amazon.Lambda.Tools il est déjà installé, assurez-vous de disposer de la dernière version.

```
dotnet tool update -g Amazon.Lambda.Tools
```

7. Amazon.Lambda.Tools Utilisez-le pour créer l'image Docker, la transférer vers un nouveau référentiel Amazon ECR et déployer la fonction Lambda.

   Pour `--function-role`, indiquez le nom du rôle, et non l'Amazon Resource Name (ARN), du rôle d'exécution de la fonction. Par exemple : `lambda-role`.

   ```
   dotnet lambda deploy-function MyFunction --function-role lambda-role
   ```

   Pour plus d'informations sur l'extension Amazon.Lambda.Tools .NET CLI, consultez le référentiel AWS Extensions for .NET CLI sur GitHub.
8. Invoquer la fonction.

   ```
   dotnet lambda invoke-function MyFunction --payload "Testing the function"
   ```

   Si tout réussit, vous devez voir ce qui suit :

   ```
   Payload:
   "TESTING THE FUNCTION"

   Log Tail:
   START RequestId: id Version: $LATEST
   END RequestId: id
   REPORT RequestId: id  Duration: 0.99 ms       Billed Duration: 1 ms         Memory
    Size: 256 MB     Max Memory Used: 12 MB
   ```
9. Supprimez la fonction Lambda.

   ```
   dotnet lambda delete-function MyFunction
   ```

Compiler le code de la fonction d'événement Lambda .NET dans un format d'exécution natif

.NET 8 prend en charge la compilation anticipée (AOT) native. Avec la compilation anticipée native, vous pouvez compiler le code de votre fonction Lambda dans un format d'environnement d'exécution natif, ce qui élimine la nécessité de compiler le code .NET au moment de l'exécution. La compilation anticipée native peut réduire le temps de démarrage à froid des fonctions Lambda que vous écrivez en .NET. Pour plus d'informations, consultez Présentation de l'environnement d'exécution .NET 8 AWS Lambda sur le AWS Compute Blog.

Sections

- Le fichier d'exécution Lambda
- Conditions préalables
- Prise en main
- Sérialisation
- Réduction
- Résolution des problèmes

Le fichier d'exécution Lambda

Pour déployer une fonction Lambda créée avec une compilation AOT native, utilisez l'environnement d'exécution Lambda géré de .NET 8. Cet environnement d'exécution prend en charge l'utilisation des architectures x86_64 et arm64.

Lorsque vous déployez une fonction Lambda .NET sans utiliser AOT, votre application est d'abord compilée en code de langage intermédiaire (IL). Au moment de l'environnement d'exécution, le compilateur JIT (just-in-time) de l'environnement d'exécution Lambda prend le code IL et le compile en code machine selon les besoins. Avec une fonction Lambda compilée à l'avance avec l'AOT native, vous compilez votre code en code machine lorsque vous déployez votre fonction, de sorte que vous ne dépendez pas de l'environnement d'exécution .NET ou du kit SDK dans l'environnement d'exécution Lambda pour compiler votre code avant qu'il ne s'exécute.

L'une des limites de l'AOT est que le code de votre application doit être compilé dans un environnement doté du même système d'exploitation Amazon Linux 2023 (AL2023) que celui utilisé par l'environnement d'exécution .NET 8. La CLI Lambda .NET fournit une fonctionnalité permettant de compiler votre application dans un conteneur Docker à l'aide d'une image AL2023.

Pour éviter d'éventuels problèmes de compatibilité entre architectures, nous vous recommandons vivement de compiler votre code dans un environnement doté de la même architecture de processeur que celle que vous avez configurée pour votre fonction. Pour en savoir plus sur les limites de la compilation entre architectures, consultez Cross-compilationla documentation Microsoft .NET.

Conditions préalables

Docker

Pour utiliser l'AOT native, votre code de fonction doit être compilé dans un environnement doté du même système d'exploitation AL2023 que l'environnement d'exécution .NET 8. Les commandes de la CLI .NET des sections suivantes utilisent Docker pour développer et construire des fonctions Lambda dans un environnement AL2023.

Kit SDK .NET 8

La compilation AOT native est une fonctionnalité de .NET 8. Vous devez installer le kit SDK .NET 8 sur votre machine de compilation, et pas seulement l'environnement d'exécution.

Amazon.Lambda.Tools

Pour créer vos fonctions Lambda, utilisez l'Amazon.Lambda.Tools extension outils globaux .NET. Pour installer Amazon.Lambda.Tools, exécutez la commande suivante :

```
dotnet tool install -g Amazon.Lambda.Tools
```

Pour plus d'informations sur l'extension Amazon.Lambda.Tools .NET CLI, consultez le référentiel AWS Extensions for .NET CLI sur GitHub.

Amazon.Lambda.Templates

Pour générer le code de votre fonction Lambda, utilisez le Amazon.Lambda.Templates NuGet package. Pour installer ce package de modèle, exécutez la commande suivante :

```
dotnet new install Amazon.Lambda.Templates
```

Prise en main

La CLI globale .NET et le AWS Serverless Application Model (AWS SAM) fournissent tous deux des modèles de démarrage pour créer des applications utilisant l'AOT natif. Pour créer votre première fonction Lambda à l'aide de la compilation anticipée native, suivez les étapes décrites dans les instructions suivantes.

Pour initialiser et déployer une fonction d'événement Lambda native compilée par AOT

1. Initialisez un nouveau projet en utilisant le modèle de la compilation anticipée native, puis naviguez dans le répertoire contenant les fichiers créés `.cs` et `.csproj`. Dans cet exemple, nous allons nommer notre fonction `NativeAotSample`.

   ```
   dotnet new lambda.NativeAOT -n NativeAotSample
   cd ./NativeAotSample/src/NativeAotSample
   ```

   Le fichier créé `Function.cs` par le modèle de la compilation anticipée native contient le code de fonction suivant.

   ```
   using Amazon.Lambda.Core;
   using Amazon.Lambda.RuntimeSupport;
   using Amazon.Lambda.Serialization.SystemTextJson;
   using System.Text.Json.Serialization;

   namespace NativeAotSample;

   public class Function
   {
       /// <summary>
       /// The main entry point for the Lambda function. The main function is called
    once during the Lambda init phase. It
       /// initializes the .NET Lambda runtime client passing in the function handler
    to invoke for each Lambda event and
       /// the JSON serializer to use for converting Lambda JSON format to the .NET
    types.
       /// </summary>
       private static async Task Main()
       {
           Func<string, ILambdaContext, string> handler = FunctionHandler;
           await LambdaBootstrapBuilder.Create(handler, new
    SourceGeneratorLambdaJsonSerializer<LambdaFunctionJsonSerializerContext>())
               .Build()
               .RunAsync();
       }

       /// <summary>
       /// A simple function that takes a string and does a ToUpper.
       ///
   ```

```
    /// To use this handler to respond to an AWS event, reference the appropriate
 package from
    /// https://github.com/aws/aws-lambda-dotnet#events
    /// and change the string input parameter to the desired event type. When the
 event type
    /// is changed, the handler type registered in the main method needs to be
 updated and the LambdaFunctionJsonSerializerContext
    /// defined below will need the JsonSerializable updated. If the return type
 and event type are different then the
    /// LambdaFunctionJsonSerializerContext must have two JsonSerializable
 attributes, one for each type.
    ///
    // When using Native AOT extra testing with the deployed Lambda functions is
 required to ensure
    // the libraries used in the Lambda function work correctly with Native AOT. If
 a runtime
    // error occurs about missing types or methods the most likely solution will be
 to remove references to trim-unsafe
    // code or configure trimming options. This sample defaults to partial TrimMode
 because currently the AWS
    // SDK for .NET does not support trimming. This will result in a larger
 executable size, and still does not
    // guarantee runtime trimming errors won't be hit.
    /// </summary>
    /// <param name="input"></param>
    /// <param name="context"></param>
    /// <returns></returns>
    public static string FunctionHandler(string input, ILambdaContext context)
    {
        return input.ToUpper();
    }
}

/// <summary>
/// This class is used to register the input event and return type for the
 FunctionHandler method with the System.Text.Json source generator.
/// There must be a JsonSerializable attribute for each type used as the input and
 return type or a runtime error will occur
/// from the JSON serializer unable to find the serialization information for
 unknown types.
/// </summary>
[JsonSerializable(typeof(string))]
public partial class LambdaFunctionJsonSerializerContext : JsonSerializerContext
{
```

```
    // By using this partial class derived from JsonSerializerContext, we can
 generate reflection free JSON Serializer code at compile time
    // which can deserialize our class and properties. However, we must attribute
 this class to tell it what types to generate serialization code for.
    // See https://docs.microsoft.com/en-us/dotnet/standard/serialization/system-
text-json-source-generation
```

La compilation anticipée native permet de compiler votre application en un seul fichier binaire natif. Le point d'entrée de ce fichier binaire est la méthode `static Main`. Dans `static Main`, l'exécution Lambda est amorcée et la méthode `FunctionHandler` est configurée. Dans le cadre de l'amorçage de l'exécution, un sérialiseur généré par la source est configuré à l'aide de `new SourceGeneratorLambdaJsonSerializer<LambdaFunctionJsonSerializerContext>()`

2. Pour déployer votre application sur Lambda, assurez-vous que Docker est en cours d'exécution dans votre environnement local et exécutez la commande suivante.

```
dotnet lambda deploy-function
```

En arrière plan, la CLI globale .NET télécharge une image Docker AL2023 et compile le code de votre application à l'intérieur d'un conteneur en cours d'exécution. Le fichier binaire compilé est renvoyé vers votre système de fichiers local avant d'être déployé sur Lambda.

3. Testez votre fonction en exécutant la commande suivante. Remplacez `<FUNCTION_NAME>` par le nom que vous avez choisi pour votre fonction dans l'assistant de déploiement.

```
dotnet lambda invoke-function <FUNCTION_NAME> --payload "hello world"
```

La réponse de la CLI comprend des détails sur les performances pour le démarrage à froid (durée d'initialisation) et la durée totale d'exécution de l'invocation de la fonction.

4. Pour supprimer les AWS ressources que vous avez créées en suivant les étapes précédentes, exécutez la commande suivante. Remplacez `<FUNCTION_NAME>` par le nom que vous avez choisi pour votre fonction dans l'assistant de déploiement. En supprimant AWS les ressources que vous n'utilisez plus, vous évitez que des frais inutiles ne soient facturés à votre Compte AWS compte.

```
dotnet lambda delete-function <FUNCTION_NAME>
```

Sérialisation

Pour déployer des fonctions sur Lambda à l'aide de la compilation anticipée native, le code de votre fonction doit utiliser la sérialisation générée par la source. Au lieu d'utiliser la réflexion au moment de l'exécution pour rassembler les métadonnées nécessaires à l'accès aux propriétés des objets pour la sérialisation, les générateurs de sources génèrent des fichiers sources C# qui sont compilés lorsque vous créez votre application. Pour configurer correctement le sérialiseur généré par la source, assurez-vous d'inclure tous les objets d'entrée et de sortie utilisés par votre fonction, ainsi que tous les types personnalisés. Par exemple, une fonction Lambda qui reçoit des événements d'API Gateway pour une API REST et renvoie un type de `Product` personnalisé inclurait un sérialiseur défini comme suit.

```
[JsonSerializable(typeof(APIGatewayProxyRequest))]
[JsonSerializable(typeof(APIGatewayProxyResponse))]
[JsonSerializable(typeof(Product))]
public partial class CustomSerializer : JsonSerializerContext
{
}
```

Réduction

La compilation anticipée native permet de réduire le code de votre application dans le cadre de la compilation afin de s'assurer que le fichier binaire est aussi petit que possible. .NET 8 pour Lambda offre une meilleure prise en charge du découpage par rapport aux versions précédentes de .NET. La prise en charge a été ajoutée aux bibliothèques d'environnement d'exécution Lambda, au kit SDK AWS .NET, aux annotations .NET Lambda et à .NET 8 lui-même.

Ces améliorations offrent la possibilité d'éliminer les avertissements de découpage au moment de la création, mais .NET n'est jamais totalement sûr pour le découpage. Cela signifie que les parties des bibliothèques sur lesquelles repose votre fonction peuvent être supprimées lors de l'étape de compilation. Vous pouvez gérer cela en le définissant `TrimmerRootAssemblies` dans le cadre de votre fichier `.csproj`, comme indiqué dans l'exemple suivant.

```
<ItemGroup>
    <TrimmerRootAssembly Include="AWSSDK.Core" />
    <TrimmerRootAssembly Include="AWSXRayRecorder.Core" />
    <TrimmerRootAssembly Include="AWSXRayRecorder.Handlers.AwsSdk" />
    <TrimmerRootAssembly Include="Amazon.Lambda.APIGatewayEvents" />
    <TrimmerRootAssembly Include="bootstrap" />
    <TrimmerRootAssembly Include="Shared" />
```

```
</ItemGroup>
```

Notez que lorsque vous recevez un avertissement de découpage, l'ajout de la classe qui génère l'avertissement `TrimmerRootAssembly` risque de ne pas résoudre le problème. Un avertissement de découpage indique que la classe essaie d'accéder à une autre classe qui ne peut être déterminée avant l'exécution. Pour éviter les erreurs d'exécution, ajoutez cette deuxième classe à `TrimmerRootAssembly`.

Pour en savoir plus sur la gestion des avertissements de découpage, consultez Introduction aux avertissements de découpage dans la documentation Microsoft .NET.

Résolution des problèmes

Erreur : la compilation Cross-OS native n'est pas prise en charge.

> Votre version de l'outil global .NET Core Amazon.Lambda.Tools n'est pas à jour. Mettez à jour vers la dernière version et réessayez.

Docker : l'image du système d'exploitation « linux » ne peut pas être utilisée sur cette plateforme.

> Docker sur votre système est configuré pour utiliser des conteneurs Windows. Passez aux conteneurs Linux pour exécuter l'environnement de création anticipée native.

Pour plus d'informations sur les erreurs courantes, consultez le référentiel AWS NativeAOT pour .NET sur. GitHub

Utilisation de l'objet de contexte Lambda pour récupérer les informations de la fonction d'événement C#

Lorsque Lambda exécute votre fonction, il transmet un objet de contexte au gestionnaire. Cet objet fournit les propriétés avec des informations sur l'appel, la fonction et l'environnement d'exécution.

Propriétés du contexte

- `FunctionName` – Nom de la fonction Lambda.
- `FunctionVersion` – Version de la fonction.
- `InvokedFunctionArn` – Amazon Resource Name (ARN) utilisé pour appeler la fonction. Indique si l'appelant a spécifié un numéro de version ou un alias.
- `MemoryLimitInMB` – Quantité de mémoire allouée à la fonction.
- `AwsRequestId` – Identifiant de la demande d'invocation.
- `LogGroupName` – Groupe de journaux pour la fonction.
- `LogStreamName` – Flux de journal de l'instance de fonction.
- `RemainingTime` (`TimeSpan`) – Nombre de millisecondes restant avant l'expiration de l'exécution.
- `Identity` – (applications mobiles) Informations sur l'identité Amazon Cognito qui a autorisé la demande.
- `ClientContext` – (applications mobiles) Contexte client fourni à Lambda par l'application client.
- `Logger` L'objet enregistreur d'événements pour la fonction.

Vous pouvez utiliser les informations contenues dans l'objet `ILambdaContext` pour générer des informations sur l'invocation de votre fonction à des fins de contrôle. Le code suivant montre comment ajouter des informations contextuelles à un cadre de journalisation structuré. Dans cet exemple, la fonction ajoute `AwsRequestId` aux sorties du journal. La fonction utilise également la propriété `RemainingTime` pour annuler une tâche en vol si le délai d'attente de la fonction Lambda est sur le point d'être atteint.

```
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSerializer

namespace GetProductHandler;

public class Function
{
```

```
    private readonly IDatabaseRepository _repo;

    public Function()
    {
        this._repo = new DatabaseRepository();
    }

    public async Task<APIGatewayProxyResponse> FunctionHandler(APIGatewayProxyRequest
 request, ILambdaContext context)
    {
        Logger.AppendKey("AwsRequestId", context.AwsRequestId);

        var id = request.PathParameters["id"];

        using var cts = new CancellationTokenSource();

        try
        {
            cts.CancelAfter(context.RemainingTime.Add(TimeSpan.FromSeconds(-1)));

            var databaseRecord = await this._repo.GetById(id, cts.Token);

            return new APIGatewayProxyResponse
            {
                StatusCode = (int)HttpStatusCode.OK,
                Body = JsonSerializer.Serialize(databaseRecord)
            };
        }
        catch (Exception ex)
        {
            return new APIGatewayProxyResponse
            {
                StatusCode = (int)HttpStatusCode.InternalServerError,
                Body = JsonSerializer.Serialize(new { error = ex.Message })
            };
        }
        finally
        {
            cts.Cancel();
        }
    }
}
```

Enregistrez et surveillez les fonctions des événements Lambda C#

AWS Lambda surveille automatiquement les fonctions Lambda et envoie des entrées de journal à Amazon. CloudWatch Votre fonction Lambda est fournie avec un groupe de CloudWatch journaux Logs et un flux de journaux pour chaque instance de votre fonction. L'environnement d'exécution Lambda envoie des détails sur chaque invocation et d'autres sorties provenant du code de votre fonction au flux de journaux. Pour plus d'informations sur CloudWatch les journaux, consultezEnvoi des journaux des fonctions d'événements Lambda aux journaux CloudWatch.

Sections

- Création d'une fonction qui renvoie des journaux
- Utilisation des contrôles de journalisation avancés de Lambda avec .NET
- Outils de journalisation et bibliothèques supplémentaires
- Utilisation de Powertools pour AWS Lambda (.NET) et AWS SAM pour une journalisation structurée
- Affichage des journaux dans la console Lambda
- Afficher les journaux dans la CloudWatch console
- Afficher les journaux à l'aide du AWS Command Line Interface (AWS CLI)
- Suppression de journaux

Création d'une fonction qui renvoie des journaux

Pour générer des journaux à partir de votre code de fonction, vous pouvez utiliser l'objet ILambdaLoggeron the context, les méthodes de la classe Console ou toute bibliothèque de journalisation qui écrit dans `stdout` ou`stderr`.

L'environnement d'exécution .NET enregistre les lignes `START`, `END` et `REPORT` pour chaque invocation. La ligne de rapport fournit les détails suivants.

Champs de données de la ligne REPORT

- RequestId— L'identifiant de demande unique pour l'invocation.
- Duration – Temps que la méthode de gestion du gestionnaire de votre fonction a consacré au traitement de l'événement.
- Billed Duration : temps facturé pour l'invocation.
- Memory Size – Quantité de mémoire allouée à la fonction.

- Max Memory Used – Quantité de mémoire utilisée par la fonction. Lorsque les appels partagent un environnement d'exécution, Lambda indique la mémoire maximale utilisée pour toutes les invocations. Ce comportement peut entraîner une valeur signalée plus élevée que prévu.
- Init Duration : pour la première requête servie, temps qu'il a pris à l'exécution charger la fonction et exécuter le code en dehors de la méthode du gestionnaire.
- XRAY TraceId — Pour les demandes suivies, l'ID de AWS X-Ray trace.
- SegmentId— Pour les demandes suivies, l'ID X-Ray du segment.
- Sampled – Pour les demandes suivies, résultat de l'échantillonnage.

Utilisation des contrôles de journalisation avancés de Lambda avec .NET

Pour mieux contrôler la manière dont les journaux de vos fonctions sont capturés, traités et consommés, vous pouvez configurer les options de journalisation suivantes pour les environnements d'exécution .NET pris en charge :

- Format de journal : choisissez entre le format texte brut et le format JSON structuré pour les journaux de votre fonction
- Niveau du journal : pour les journaux au format JSON, choisissez le niveau de détail des journaux auxquels Lambda envoie CloudWatch, par exemple ERROR, DEBUG ou INFO
- Groupe de journaux : choisissez le groupe de CloudWatch journaux auquel votre fonction envoie les journaux

Pour plus d'informations sur ces options de journalisation et pour savoir comment configurer votre fonction pour les utiliser, consultez the section called "Configuration de contrôles de journalisation avancés pour les fonctions d'événement Lambda".

Pour utiliser le format de journal et les options de niveau de journal avec vos fonctions Lambda .NET, consultez les instructions des sections suivantes.

Utilisation du format de journal JSON structuré avec .NET

Si vous sélectionnez JSON pour le format de journal de votre fonction, Lambda envoie les résultats des journaux ILambdaLoggersous forme de JSON structuré. Chaque objet de journal JSON contient au moins cinq paires clé-valeur avec les clés suivantes :

- `"timestamp"` - heure à laquelle le message de journal a été généré
- `"level"` - niveau de journalisation attribué au message

- `"requestId"` - identifiant unique de la demande pour l'invocation de la fonction
- `"traceId"` : la variable d'environnement `_X_AMZN_TRACE_ID`
- `"message"` - contenu du message de journal

L'instance `ILambdaLogger` peut ajouter des paires clé-valeur supplémentaires, par exemple lors de la journalisation des exceptions. Vous pouvez également fournir vos propres paramètres supplémentaires, comme décrit dans la section the section called "Customer-provided paramètres du journal".

> **Note**
>
> Si votre code utilise déjà une autre bibliothèque de journalisation pour générer des JSON-formatted journaux, assurez-vous que le format de journal de votre fonction est défini sur du texte brut. Si vous définissez le format de journal sur JSON, les sorties de votre journal sont codées deux fois.

L'exemple de commande de journalisation suivant montre comment écrire un message de journal de niveau `INFO`.

Example Code de journalisation .NET

```
context.Logger.LogInformation("Fetching cart from database");
```

Vous pouvez également utiliser une méthode de journal générique qui prend le niveau de journal comme argument, comme le montre l'exemple suivant.

```
context.Logger.Log(LogLevel.Information, "Fetching cart from database");
```

La sortie du journal par ces exemples d'extraits de code serait capturée dans CloudWatch Logs comme suit :

Example Enregistrement de journaux JSON

```
{
    "timestamp": "2025-09-07T01:30:06.977Z",
    "level": "Information",
```

```
    "requestId": "8f711428-7e55-46f9-ae88-2a65d4f85fc5",
    "traceId": "1-6408af34-50f56f5b5677a7d763973804",
    "message": "Fetching cart from database"
}
```

> **Note**
>
> Si vous configurez le format de journal de votre fonction pour utiliser du texte brut plutôt que du JSON, le niveau de journal capturé dans le message suit la convention de Microsoft qui consiste à utiliser une étiquette à quatre caractères. Par exemple, un niveau de journalisation `Debug` est représenté dans le message sous la forme `dbug`.
> Lorsque vous configurez votre fonction pour utiliser des journaux au format JSON, le niveau de journal capturé dans le journal utilise l'étiquette complète, comme indiqué dans l'exemple d'enregistrement de journal JSON.

Si vous n'attribuez aucun niveau à la sortie de votre journal, Lambda lui attribue automatiquement le niveau INFO.

Exceptions de journalisation au format JSON

Lorsque vous utilisez la journalisation JSON structurée avec `ILambdaLogger`, vous pouvez journaliser les exceptions dans votre code, comme indiqué dans l'exemple suivant.

Example utilisation de la journalisation des exceptions

```
try
{
    connection.ExecuteQuery(query);
}
catch(Exception e)
{
    context.Logger.LogWarning(e, "Error executing query");
}
```

Le format de journal généré par ce code est illustré dans l'exemple de JSON suivant. Notez que la propriété `message` du JSON est renseignée à l'aide de l'argument message fourni dans l'appel `LogWarning`, tandis que la propriété `errorMessage` provient de la propriété `Message` de l'exception elle-même.

Example Enregistrement de journaux JSON

```
{
    "timestamp": "2025-09-07T01:30:06.977Z",
    "level": "Warning",
    "requestId": "8f711428-7e55-46f9-ae88-2a65d4f85fc5",
    "traceId": "1-6408af34-50f56f5b5677a7d763973804",
    "message": "Error executing query",
    "errorType": "System.Data.SqlClient.SqlException",
    "errorMessage": "Connection closed",
    "stackTrace": ["<call exception.StackTrace>"]
}
```

Si le format de journalisation de votre fonction est défini sur JSON, Lambda produit également des messages de JSON-formatted journal lorsque votre code génère une exception non détectée. L'exemple d'extrait de code et de message de journal suivants montre comment les exceptions non détectées sont journalisées.

Example code d'exception

```
throw new ApplicationException("Invalid data");
```

Example Enregistrement de journaux JSON

```
{
    "timestamp": "2025-09-07T01:30:06.977Z",
    "level": "Error",
    "requestId": "8f711428-7e55-46f9-ae88-2a65d4f85fc5",
    "traceId": "1-6408af34-50f56f5b5677a7d763973804",
    "message": "Invalid data",
    "errorType": "System.ApplicationException",
    "errorMessage": "Invalid data",
    "stackTrace": ["<call exception.StackTrace>"]
}
```

Customer-provided paramètres du journal

Avec les messages de JSON-formatted journal, vous pouvez fournir des paramètres de journal supplémentaires et les inclure dans le journal`message`. L'exemple d'extrait de code suivant montre une commande permettant d'ajouter deux paramètres fournis par l'utilisateur et étiquetés

`retryAttempt` et `uri`. Dans l'exemple, la valeur de ces paramètres provient des arguments `retryAttempt` et `uriDestination` transmis à la commande de journalisation.

Example Commande de journalisation JSON avec paramètres supplémentaires

```
context.Logger.LogInformation("Starting retry {retryAttempt} to make GET request to
 {uri}", retryAttempt, uriDestination);
```

Le message du journal généré par cette commande est illustré dans l'exemple de fichier JSON suivant.

Example Enregistrement de journaux JSON

```
{
    "timestamp": "2025-09-07T01:30:06.977Z",
    "level": "Information",
    "requestId": "8f711428-7e55-46f9-ae88-2a65d4f85fc5",
    "traceId": "1-6408af34-50f56f5b5677a7d763973804",
    "message": "Starting retry 1 to make GET request to http://example.com/",
    "retryAttempt": 1,
    "uri": "http://example.com/"
}
```

Tip

Vous pouvez également utiliser des propriétés de positionnement plutôt que des noms lorsque vous spécifiez des paramètres supplémentaires. Par exemple, dans l'exemple précédent, la commande peut également être écrite comme suit :

```
context.Logger.LogInformation("Starting retry {0} to make GET request to {1}",
 retryAttempt, uriDestination);
```

Notez que lorsque vous fournissez des paramètres de journalisation supplémentaires, Lambda les capture en tant que propriétés de premier niveau dans l'enregistrement de journal JSON. Cette approche diffère de certaines bibliothèques de journalisation .NET populaires `Serilog`, telles que celles qui capturent des paramètres supplémentaires dans un objet enfant distinct.

Si l'argument que vous fournissez pour un paramètre supplémentaire est un objet complexe, Lambda utilise par défaut la méthode `ToString()` pour fournir la valeur. Pour indiquer qu'un argument doit

être sérialisé au format JSON, utilisez le préfixe `@` tel qu'illustré dans l'extrait de code suivant. Dans cet exemple, `User` est un objet doté de propriétés `FirstName` et `LastName`.

Example Commande de journalisation JSON avec objet sérialisé JSON

```
context.Logger.LogInformation("User {@user} logged in", User);
```

Le message du journal généré par cette commande est illustré dans l'exemple de fichier JSON suivant.

Example Enregistrement de journaux JSON

```
{
    "timestamp": "2025-09-07T01:30:06.977Z",
    "level": "Information",
    "requestId": "8f711428-7e55-46f9-ae88-2a65d4f85fc5",
    "traceId": "1-6408af34-50f56f5b5677a7d763973804",
    "message": "User {@user} logged in",
    "user":
    {
        "FirstName": "John",
        "LastName": "Doe"
    }
}
```

Si l'argument d'un paramètre supplémentaire est un tableau ou implémente `IList` ou `IDictionary`, alors Lambda ajoute l'argument au message de journal JSON sous forme de tableau, comme indiqué dans l'exemple d'enregistrement de journal JSON suivant. Dans cet exemple, `{users}` prend un argument `IList` contenant des instances de la propriété `User` au même format que dans l'exemple précédent. Lambda le convertit cet `IList` en tableau, chaque valeur étant créée à l'aide de la méthode `ToString`.

Example Enregistrement de journal JSON avec un **`argument IList`**

```
{
    "timestamp": "2025-09-07T01:30:06.977Z",
    "level": "Information",
    "requestId": "8f711428-7e55-46f9-ae88-2a65d4f85fc5",
    "traceId": "1-6408af34-50f56f5b5677a7d763973804",
    "message": "{users} have joined the group",
    "users":
```

```
    [
        "Rosalez, Alejandro",
        "Stiles, John"
    ]
}
```

Vous pouvez également sérialiser la liste au format JSON en utilisant le préfixe `@` dans votre commande de journalisation. Dans l'exemple d'enregistrement de journal JSON suivant, la propriété `users` est sérialisée au format JSON.

Example Enregistrement de journal JSON avec un argument **`IList`** sérialisé au format JSON

```
{
    "timestamp": "2025-09-07T01:30:06.977Z",
    "level": "Information",
    "requestId": "8f711428-7e55-46f9-ae88-2a65d4f85fc5",
    "traceId": "1-6408af34-50f56f5b5677a7d763973804",
    "message": "{@users} have joined the group",
    "users":
    [
        {
            "FirstName": "Alejandro",
            "LastName": "Rosalez"
        },
        {
            "FirstName": "John",
            "LastName": "Stiles"
        }
    ]
}
```

Utilisation du filtrage au niveau du journal avec .NET

En configurant le filtrage au niveau des journaux, vous pouvez choisir de n'envoyer que les journaux d'un certain niveau de détail ou inférieur à CloudWatch Logs. Pour savoir comment configurer le filtrage de niveau journal de votre fonction, consultez the section called “Log-level filtrage”.

AWS Lambda Pour filtrer vos messages de journal par niveau de journal, vous pouvez soit utiliser des journaux au format JSON, soit utiliser les `Console` méthodes .NET pour générer des messages de journal. Pour créer des journaux au format JSON, configurez le type de journal de votre fonction sur JSON et utilisez l'instance `ILambdaLogger`.

Avec JSON-formatted les journaux, Lambda filtre les sorties de vos journaux à l'aide de la paire clé-valeur « niveau » de l'objet JSON décrit dans. the section called “Utilisation du format de journal JSON structuré avec .NET”

Si vous utilisez les `Console` méthodes .NET pour écrire des messages dans CloudWatch Logs, Lambda applique les niveaux de journalisation à vos messages comme suit :

- Console.WriteLine méthode - Lambda applique un niveau de journalisation de `INFO`
- Console.Error méthode - Lambda applique un niveau de journalisation de `ERROR`

Lorsque vous configurez votre fonction pour utiliser le filtrage au niveau des journaux, vous devez sélectionner parmi les options suivantes le niveau de journaux que Lambda doit envoyer à Logs. CloudWatch Notez le mappage des niveaux de journalisation utilisés par Lambda avec les niveaux Microsoft standard utilisés par l’attribut .NET `ILambdaLogger`.

Niveau du journal de Lambda	Niveau Microsoft équivalent	Utilisation standard
TRACE (le plus détaillé)	Suivi	Les informations les plus précises utilisées pour tracer le chemin d’exécution de votre code
DEBUG	Débogage	Informations détaillées pour le débogage du système
INFO	Informations	Messages qui enregistrent le fonctionnement normal de votre fonction
WARN	Avertissement	Messages concernant des erreurs potentielles susceptib les d'entraîner un comportem ent inattendu si elles ne sont pas traitées
ERROR	Erreur	Messages concernant les problèmes qui empêchent le

Niveau du journal de Lambda	Niveau Microsoft équivalent	Utilisation standard
		code de fonctionner comme prévu
FATAL (moindre détail)	Critique	Messages relatifs à des erreurs graves entraînant l'arrêt du fonctionnement de l'application

Lambda envoie des journaux correspondant au niveau de détail sélectionné et inférieur à. CloudWatch Par exemple, si vous configurez un niveau de journalisation WARN, Lambda envoie des journaux correspondant aux niveaux WARN, ERROR et FATAL.

Outils de journalisation et bibliothèques supplémentaires

Powertools for AWS Lambda (.NET) est une boîte à outils destinée aux développeurs qui permet de mettre en œuvre les meilleures pratiques sans serveur et d'accroître la rapidité des développeurs. L'utilitaire Logging (français non garanti) fournit un enregistreur optimisé pour Lambda qui inclut des informations supplémentaires sur le contexte de fonction pour toutes vos fonctions avec une sortie structurée en JSON. Utilisez cet utilitaire pour effectuer les opérations suivantes :

- Capturer les champs clés du contexte Lambda, démarrer à froid et structurer la sortie de la journalisation sous forme de JSON
- Journaliser les événements d'invocation Lambda lorsque cela est demandé (désactivé par défaut)
- Imprimer tous les journaux uniquement pour un pourcentage d'invocations via l'échantillonnage des journaux (désactivé par défaut)
- Ajouter des clés supplémentaires au journal structuré à tout moment
- Utiliser un formateur de journaux personnalisé (Apportez votre propre formateur) pour produire des journaux dans une structure compatible avec le RFC de journalisation de votre organisation

Utilisation de Powertools pour AWS Lambda (.NET) et AWS SAM pour une journalisation structurée

Suivez les étapes ci-dessous pour télécharger, créer et déployer un exemple d'application Hello World C# avec des modules Powertools pour AWS Lambda (.NET) intégrés à l'aide du. AWS SAM Cette application met en œuvre un backend API de base et utilise Powertools pour émettre des journaux, des métriques et des traces. Elle se compose d'un point de terminaison Amazon API

Gateway et d'une fonction Lambda. Lorsque vous envoyez une requête GET au point de terminaison API Gateway, la fonction Lambda appelle, envoie des journaux et des métriques au format métrique intégré à CloudWatch, et envoie des traces à. AWS X-Ray La fonction renvoie un message `hello world`.

Conditions préalables

Pour exécuter la procédure indiquée dans cette section, vous devez satisfaire aux exigences suivantes :

- .NET 8
- AWS CLI version 2
- AWS SAM CLI version 1.75 ou ultérieure. Si vous disposez d'une ancienne version de la AWS SAM CLI, consultez la section Mise à niveau de la AWS SAM CLI.

Déployer un échantillon AWS SAM vigie

1. Initialisez l'application à l'aide du TypeScript modèle Hello World.

```
sam init --app-template hello-world-powertools-dotnet --name sam-app --package-type
 Zip --runtime dotnet6 --no-tracing
```

2. Créez l'application.

```
cd sam-app && sam build
```

3. Déployez l'application.

```
sam deploy --guided
```

4. Suivez les invites à l'écran. Appuyez sur `Enter` pour accepter les options par défaut fournies dans l'expérience interactive.

> **Note**
>
> Car l'autorisation n'a HelloWorldFunction peut-être pas été définie, est-ce que ça va ? , assurez-vous de participery.

5. Obtenez l'URL de l'application déployée :

```
aws cloudformation describe-stacks --stack-name sam-app --query
 'Stacks[0].Outputs[?OutputKey==`HelloWorldApi`].OutputValue' --output text
```

6. Invoquez le point de terminaison de l'API :

```
curl -X GET <URL_FROM_PREVIOUS_STEP>
```

En cas de succès, vous obtiendrez cette réponse :

```
{"message":"hello world"}
```

7. Pour obtenir les journaux de la fonction, exécutez sam logs. Pour en savoir plus, consultez Utilisation des journaux dans le Guide du développeur AWS Serverless Application Model .

```
sam logs --stack-name sam-app
```

La sortie du journal se présente comme suit :

```
2025/02/20/[$LATEST]4eaf8445ba7a4a93b999cb17fbfbecd8
 2025-09-20T14:15:27.988000 INIT_START Runtime Version:
 dotnet:6.v13        Runtime Version ARN: arn:aws:lambda:ap-
southeast-2::runtime:699f346a05dae24c58c45790bc4089f252bf17dae3997e79b17d939a288aa1ec
2025/02/20/[$LATEST]4eaf8445ba7a4a93b999cb17fbfbecd8 2025-09-20T14:15:28.229000
 START RequestId: bed25b38-d012-42e7-ba28-f272535fb80e Version: $LATEST
2025/02/20/[$LATEST]4eaf8445ba7a4a93b999cb17fbfbecd8 2025-09-20T14:15:29.259000
 2025-09-20T14:15:29.201Z        bed25b38-d012-42e7-ba28-f272535fb80e    info
   {"_aws":{"Timestamp":1676902528962,"CloudWatchMetrics":[{"Namespace":"sam-
app-logging","Metrics":[{"Name":"ColdStart","Unit":"Count"}],"Dimensions":
[["FunctionName"],["Service"]]}]},"FunctionName":"sam-app-HelloWorldFunction-
haKIoVeose2p","Service":"PowertoolsHelloWorld","ColdStart":1}
2025/02/20/[$LATEST]4eaf8445ba7a4a93b999cb17fbfbecd8 2025-09-20T14:15:30.479000
 2025-09-20T14:15:30.479Z        bed25b38-d012-42e7-ba28-f272535fb80e    info
 {"ColdStart":true,"XrayTraceId":"1-63f3807f-5dbcb9910c96f50742707542","CorrelationId":"d3d
a549-4d67b2fdc015","FunctionName":"sam-app-HelloWorldFunction-
haKIoVeose2p","FunctionVersion":"$LATEST","FunctionMemorySize":256,"FunctionArn":"arn:aws:l
southeast-2:123456789012:function:sam-app-HelloWorldFunction-
haKIoVeose2p","FunctionRequestId":"bed25b38-d012-42e7-ba28-
f272535fb80e","Timestamp":"2025-09-20T14:15:30.4602970Z","Level":"Information","Service":"P
 world API - HTTP 200"}
```

```
2025/02/20/[$LATEST]4eaf8445ba7a4a93b999cb17fbfbecd8 2025-09-20T14:15:30.599000
 2025-09-20T14:15:30.599Z        bed25b38-d012-42e7-ba28-f272535fb80e    info
   {"_aws":{"Timestamp":1676902528922,"CloudWatchMetrics":[{"Namespace":"sam-
app-logging","Metrics":[{"Name":"ApiRequestCount","Unit":"Count"}],"Dimensions":
[["Service"]]}]},"Service":"PowertoolsHelloWorld","ApiRequestCount":1}
2025/02/20/[$LATEST]4eaf8445ba7a4a93b999cb17fbfbecd8 2025-09-20T14:15:30.680000 END
 RequestId: bed25b38-d012-42e7-ba28-f272535fb80e
2025/02/20/[$LATEST]4eaf8445ba7a4a93b999cb17fbfbecd8 2025-09-20T14:15:30.680000
 REPORT RequestId: bed25b38-d012-42e7-ba28-f272535fb80e  Duration: 2450.99 ms
  Billed Duration: 2692 ms Memory Size: 256 MB     Max Memory Used: 74 MB  Init
 Duration: 240.05 ms
XRAY TraceId: 1-63f3807f-5dbcb9910c96f50742707542       SegmentId: 16b362cd5f52cba0
```

8. Il s'agit d'un point de terminaison d'API public accessible par Internet. Nous vous recommandons de supprimer le point de terminaison après un test.

```
sam delete
```

Gestion de la conservation des journaux

Les groupes de journaux ne sont pas supprimés automatiquement quand vous supprimez une fonction. Pour éviter de stocker les journaux indéfiniment, supprimez le groupe de journaux ou configurez une période de conservation après laquelle les journaux CloudWatch sont automatiquement supprimés. Pour configurer la conservation des journaux, ajoutez ce qui suit à votre AWS SAM modèle :

```
Resources:
  HelloWorldFunction:
    Type: AWS::Serverless::Function
    Properties:
      # Omitting other properties

  LogGroup:
    Type: AWS::Logs::LogGroup
    Properties:
      LogGroupName: !Sub "/aws/lambda/${HelloWorldFunction}"
      RetentionInDays: 7
```

Affichage des journaux dans la console Lambda

Vous pouvez utiliser la console Lambda pour consulter les résultats du journal après avoir invoqué une fonction d'événement Lambda.

Si votre code peut être testé à partir de l'éditeur de code intégré, vous trouverez des journaux dans les résultats d'exécution. Lorsque vous utilisez la fonctionnalité de test de la console pour appeler une fonction, vous trouverez la sortie du journal dans la section Détails.

Afficher les journaux dans la CloudWatch console

Vous pouvez utiliser la CloudWatch console Amazon pour consulter les journaux de toutes les invocations de la fonction d'événement Lambda.

Pour afficher les journaux sur la CloudWatch console

1. Ouvrez la page Groupes de journaux sur la CloudWatch console.
2. Choisissez le groupe de journaux pour votre fonction (/aws/lambda/***your-function-name***).
3. Choisissez un flux de journaux.

Chaque flux de journal correspond à une instance de votre fonction. Un flux de journal apparaît lorsque vous mettez à jour votre fonction Lambda et lorsque des instances supplémentaires sont créées pour gérer les appels simultanés. Pour trouver les journaux d'un appel spécifique, nous vous recommandons d'instrumenter votre fonction avec. AWS X-Ray X-Ray enregistre les détails de la demande et du flux de log dans la trace.

Afficher les journaux à l'aide du AWS Command Line Interface (AWS CLI)

AWS CLI Il s'agit d'un outil open source que vous pouvez utiliser pour interagir avec les AWS services à l'aide de commandes dans votre interface de ligne de commande. Pour effectuer les étapes de cette section, vous devez disposer de la version 2 de l'AWS CLI.

Vous pouvez utiliser AWS CLI pour récupérer les journaux d'une invocation à l'aide de l'option de commande `--log-type`. La réponse inclut un champ `LogResult` qui contient jusqu'à 4 Ko de journaux codés en base64 provenant de l'invocation.

Example récupérer un ID de journal

L'exemple suivant montre comment récupérer un ID de journal à partir du champ `LogResult` d'une fonction nommée `my-function`.

```
aws lambda invoke --function-name my-function out --log-type Tail
```

Vous devriez voir la sortie suivante:

```
{
    "StatusCode": 200,
    "LogResult":
 "U1RBUlQgUmVxdWVzdElkOiA4N2QwNDRiOC1mMTU0LTExZTgtOGNkYS0yOTc0YzVlNGZiMjEgVmVyc2lvb...",
    "ExecutedVersion": "$LATEST"
}
```

Example décoder les journaux

Dans la même invite de commandes, utilisez l'utilitaire `base64` pour décoder les journaux. L'exemple suivant montre comment récupérer les journaux encodés en base64 pour `my-function`.

```
aws lambda invoke --function-name my-function out --log-type Tail \
--query 'LogResult' --output text --cli-binary-format raw-in-base64-out | base64 --
decode
```

L'cli-binary-formatoption est obligatoire si vous utilisez AWS CLI la version 2. Pour faire de ce paramètre le paramètre par défaut, exécutez `aws configure set cli-binary-format raw-in-base64-out`. Pour plus d'informations, consultez les options de ligne de commande globales AWS CLI prises en charge dans le Guide de l'utilisateur AWS Command Line Interface version 2.

Vous devriez voir la sortie suivante :

```
START RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8 Version: $LATEST
"AWS_SESSION_TOKEN": "AgoJb3JpZ2luX2VjELj...", "_X_AMZN_TRACE_ID": "Root=1-5d02e5ca-
f5792818b6fe8368e5b51d50;Parent=191db58857df8395;Sampled=0"",ask/lib:/opt/lib",
END RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8
REPORT RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8  Duration: 79.67 ms      Billed
 Duration: 80 ms         Memory Size: 128 MB     Max Memory Used: 73 MB
```

L'utilitaire `base64` est disponible sous Linux, macOS et Ubuntu sous Windows. Les utilisateurs de macOS auront peut-être besoin d'utiliser `base64 -D`.

Example Script get-logs.sh

Dans la même invite de commandes, utilisez le script suivant pour télécharger les cinq derniers événements de journalisation. Le script utilise `sed` pour supprimer les guillemets du fichier de sortie

et attend 15 secondes pour permettre la mise à disposition des journaux. La sortie comprend la réponse de Lambda, ainsi que la sortie de la commande `get-log-events`.

Copiez le contenu de l'exemple de code suivant et enregistrez-le dans votre répertoire de projet Lambda sous `get-logs.sh`.

L'cli-binary-formatoption est obligatoire si vous utilisez AWS CLI la version 2. Pour faire de ce paramètre le paramètre par défaut, exécutez `aws configure set cli-binary-format raw-in-base64-out`. Pour plus d'informations, consultez les options de ligne de commande globales AWS CLI prises en charge dans le Guide de l'utilisateur AWS Command Line Interface version 2.

```
#!/bin/bash
aws lambda invoke --function-name my-function --cli-binary-format raw-in-base64-out --
payload '{"key": "value"}' out
sed -i'' -e 's/"//g' out
sleep 15
aws logs get-log-events --log-group-name /aws/lambda/my-function --log-stream-
name stream1 --limit 5
```

Example macOS et Linux (uniquement)

Dans la même invite de commande, les utilisateurs de macOS et de Linux devront peut-être exécuter la commande suivante pour s'assurer que le script est exécutable.

```
chmod -R 755 get-logs.sh
```

Example récupérer les cinq derniers événements de journal

Dans la même invite de commande, exécutez le script suivant pour obtenir les cinq derniers événements de journalisation.

```
./get-logs.sh
```

Vous devriez voir la sortie suivante:

```
{
    "StatusCode": 200,
    "ExecutedVersion": "$LATEST"
}
{
```

```
    "events": [
        {
            "timestamp": 1559763003171,
            "message": "START RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf Version:
 $LATEST\n",
            "ingestionTime": 1559763003309
        },
        {
            "timestamp": 1559763003173,
            "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tENVIRONMENT VARIABLES\r{\r  \"AWS_LAMBDA_FUNCTION_VERSION\": \"$LATEST\",
\r ...",
            "ingestionTime": 1559763018353
        },
        {
            "timestamp": 1559763003173,
            "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tEVENT\r{\r  \"key\": \"value\"\r}\n",
            "ingestionTime": 1559763018353
        },
        {
            "timestamp": 1559763003218,
            "message": "END RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf\n",
            "ingestionTime": 1559763018353
        },
        {
            "timestamp": 1559763003218,
            "message": "REPORT RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tDuration: 26.73 ms\tBilled Duration: 27 ms \tMemory Size: 128 MB\tMax Memory Used: 75
 MB\t\n",
            "ingestionTime": 1559763018353
        }
    ],
    "nextForwardToken": "f/34783877304859518393868359594929986069206639495374241795",
    "nextBackwardToken": "b/34783877303811383369537420289090800615709599058929582080"
}
```


Suppression de journaux

Les groupes de journaux ne sont pas supprimés automatiquement quand vous supprimez une fonction. Pour éviter de stocker des journaux indéfiniment, supprimez le groupe de journaux ou configurez une période de conservation à l'issue de laquelle les journaux sont supprimés automatiquement.

Instrumentation du code C# dans AWS Lambda

Lambda s'intègre pour vous aider AWS X-Ray à suivre, à déboguer et à optimiser les applications Lambda. Vous pouvez l'utiliser X-Ray pour suivre une demande lorsqu'elle parcourt les ressources de votre application, ce qui peut inclure des fonctions Lambda et AWS d'autres services.

Pour envoyer des données de suivi à X-Ray, vous pouvez utiliser l'une des trois bibliothèques du SDK :

- AWS Distro for OpenTelemetry (ADOT) — Une distribution sécurisée, prête pour la production et prise AWS en charge du SDK (OTel). OpenTelemetry
- Kit SDK AWS X-Ray pour .NET— Un SDK pour générer et envoyer des données de trace à X-Ray.
- Powertools for AWS Lambda (.NET) — Une boîte à outils pour les développeurs permettant de mettre en œuvre les meilleures pratiques sans serveur et d'accroître la rapidité des développeurs.

Chacun des SDK propose des moyens d'envoyer vos données de télémétrie au service. X-Ray Vous pouvez ensuite les utiliser X-Ray pour afficher, filtrer et obtenir des informations sur les indicateurs de performance de votre application afin d'identifier les problèmes et les opportunités d'optimisation.

> **Important**
>
> Les X-Ray et Powertools for AWS Lambda SDK font partie d'une solution d'instrumentation étroitement intégrée proposée par. AWS Les couches ADOT Lambda font partie d'une norme industrielle pour l'instrumentation de traçage qui collecte plus de données en général, mais qui peut ne pas convenir à tous les cas d'utilisation. Vous pouvez implémenter le suivi de bout en bout à l' X-Ray aide de l'une ou l'autre solution. Pour en savoir plus sur le choix entre les deux, voir Choisir entre la AWS distribution pour Open Telemetry et les SDK. X-Ray

Sections

- Utilisation de Powertools pour AWS Lambda (.NET) et AWS SAM pour le traçage
- Utilisation du X-Ray SDK pour instrumenter vos fonctions .NET
- Activation du suivi avec la console Lambda
- Activation du suivi avec l'API Lambda
- Activation du traçage avec CloudFormation
- Interprétation et X-Ray traçage

Utilisation de Powertools pour AWS Lambda (.NET) et AWS SAM pour le traçage

Suivez les étapes ci-dessous pour télécharger, créer et déployer un exemple d'application Hello World C# avec des modules Powertools pour AWS Lambda (.NET) intégrés à l'aide du. AWS SAM Cette application met en œuvre un backend API de base et utilise Powertools pour émettre des journaux, des métriques et des traces. Elle se compose d'un point de terminaison Amazon API Gateway et d'une fonction Lambda. Lorsque vous envoyez une requête GET au point de terminaison API Gateway, la fonction Lambda appelle, envoie des journaux et des métriques au format métrique intégré à CloudWatch, et envoie des traces à. AWS X-Ray La fonction renvoie un message hello world.

Conditions préalables

Pour exécuter la procédure indiquée dans cette section, vous devez satisfaire aux exigences suivantes :

- .NET 8
- AWS CLI version 2
- AWS SAM CLI version 1.75 ou ultérieure. Si vous disposez d'une ancienne version de la AWS SAM CLI, consultez la section Mise à niveau de la AWS SAM CLI.

Déployer un échantillon AWS SAM vigie

1. Initialisez l'application à l'aide du TypeScript modèle Hello World.

```
sam init --app-template hello-world-powertools-dotnet --name sam-app --package-type
 Zip --runtime dotnet6 --no-tracing
```

2. Créez l'application.

```
cd sam-app && sam build
```

3. Déployez l'application.

```
sam deploy --guided
```

4. Suivez les invites à l'écran. Appuyez sur `Enter` pour accepter les options par défaut fournies dans l'expérience interactive.

> **Note**
>
> Car l'autorisation n'a HelloWorldFunction peut-être pas été définie, est-ce que ça va ? , assurez-vous de participery.

5. Obtenez l'URL de l'application déployée :

```
aws cloudformation describe-stacks --stack-name sam-app --query
 'Stacks[0].Outputs[?OutputKey==`HelloWorldApi`].OutputValue' --output text
```

6. Invoquez le point de terminaison de l'API :

```
curl <URL_FROM_PREVIOUS_STEP>
```

En cas de succès, vous obtiendrez cette réponse :

```
{"message":"hello world"}
```

7. Pour obtenir les traces de la fonction, exécutez sam traces.

```
sam traces
```

La sortie de la trace ressemble à ceci :

```
New XRay Service Graph
  Start time: 2023-02-20 23:05:16+08:00
  End time: 2023-02-20 23:05:16+08:00
  Reference Id: 0 - AWS::Lambda - sam-app-HelloWorldFunction-pNjujb7mEoew - Edges:
 [1]
   Summary_statistics:
     - total requests: 1
     - ok count(2XX): 1
     - error count(4XX): 0
     - fault count(5XX): 0
     - total response time: 2.814
  Reference Id: 1 - AWS::Lambda::Function - sam-app-HelloWorldFunction-pNjujb7mEoew
 - Edges: []
   Summary_statistics:
     - total requests: 1
     - ok count(2XX): 1
```

```
    - error count(4XX): 0
    - fault count(5XX): 0
    - total response time: 2.429
  Reference Id: 2 - (Root) AWS::ApiGateway::Stage - sam-app/Prod - Edges: [0]
   Summary_statistics:
    - total requests: 1
    - ok count(2XX): 1
    - error count(4XX): 0
    - fault count(5XX): 0
    - total response time: 2.839
  Reference Id: 3 - client - sam-app/Prod - Edges: [2]
   Summary_statistics:
    - total requests: 0
    - ok count(2XX): 0
    - error count(4XX): 0
    - fault count(5XX): 0
    - total response time: 0

XRay Event [revision 3] at (2023-02-20T23:05:16.521000) with id
 (1-63f38c2c-270200bf1d292a442c8e8a00) and duration (2.877s)
 - 2.839s - sam-app/Prod [HTTP: 200]
   - 2.836s - Lambda [HTTP: 200]
 - 2.814s - sam-app-HelloWorldFunction-pNjujb7mEoew [HTTP: 200]
 - 2.429s - sam-app-HelloWorldFunction-pNjujb7mEoew
   - 0.230s - Initialization
   - 2.389s - Invocation
     - 0.600s - ## FunctionHandler
       - 0.517s - Get Calling IP
   - 0.039s - Overhead
```

8. Il s’agit d’un point de terminaison d’API public accessible par Internet. Nous vous recommandons de supprimer le point de terminaison après un test.

```
sam delete
```

X-Ray ne retrace pas toutes les demandes jusqu'à votre application. X-Ray applique un algorithme d'échantillonnage pour garantir l'efficacité du suivi, tout en fournissant un échantillon représentatif de toutes les demandes. Le taux d’échantillonnage est 1 demande par seconde et 5 % de demandes supplémentaires. Vous ne pouvez pas configurer le taux X-Ray d'échantillonnage pour vos fonctions.

Utilisation du X-Ray SDK pour instrumenter vos fonctions .NET

Vous pouvez instrumenter le code de gestionnaire pour enregistrer les métadonnées et suivre les appels en aval. Pour enregistrer les détails des appels que votre fonction effectue vers d'autres ressources et services, utilisez le Kit SDK AWS X-Ray pour .NET. Pour obtenir ce kit SDK, ajoutez les packages `AWSXRayRecorder` à votre fichier de projet.

```
<Project Sdk="Microsoft.NET.Sdk">
  <PropertyGroup>
    <TargetFramework>net8.0</TargetFramework>
    <GenerateRuntimeConfigurationFiles>true</GenerateRuntimeConfigurationFiles>
    <AWSProjectType>Lambda</AWSProjectType>
  </PropertyGroup>
  <ItemGroup>
    <PackageReference Include="Amazon.Lambda.Core" Version="2.1.0" />
    <PackageReference Include="Amazon.Lambda.SQSEvents" Version="2.1.0" />
    <PackageReference Include="Amazon.Lambda.Serialization.Json" Version="2.1.0" />
    <PackageReference Include="AWSSDK.Core" Version="3.7.103.24" />
    <PackageReference Include="AWSSDK.Lambda" Version="3.7.104.3" />
    <PackageReference Include="AWSXRayRecorder.Core" Version="2.13.0" />
    <PackageReference Include="AWSXRayRecorder.Handlers.AwsSdk" Version="2.11.0" />
  </ItemGroup>
</Project>
```

Il existe une gamme de packages Nuget qui fournissent une instrumentation automatique pour les AWS SDK, Entity Framework et les requêtes HTTP. Pour connaître l'ensemble des options de configuration, reportez-vous à kit SDK AWS X-Ray pour .NET dans le Guide du développeur AWS X-Ray .

Une fois que vous avez ajouté les packages Nuget de votre choix, configurez l'auto-instrumentation. La meilleure pratique consiste à effectuer cette configuration en dehors de la fonction du gestionnaire de votre fonction. Cela permet de tirer parti de la réutilisation de l'environnement d'exécution pour améliorer les performances de votre fonction. Dans l'exemple de code suivant, la `RegisterXRayForAllServices` méthode est appelée dans le constructeur de fonctions pour ajouter de l'instrumentation à tous les appels du AWS SDK.

```
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSerializer

namespace GetProductHandler;
```

```
public class Function
{
    private readonly IDatabaseRepository _repo;

    public Function()
    {
        // Add auto instrumentation for all AWS SDK calls
        // It is important to call this method before initializing any SDK clients
        AWSSDKHandler.RegisterXRayForAllServices();
        this._repo = new DatabaseRepository();
    }

    public async Task<APIGatewayProxyResponse> FunctionHandler(APIGatewayProxyRequest
 request)
    {
        var id = request.PathParameters["id"];

        var databaseRecord = await this._repo.GetById(id);

        return new APIGatewayProxyResponse
        {
            StatusCode = (int)HttpStatusCode.OK,
            Body = JsonSerializer.Serialize(databaseRecord)
        };
    }
}
```

Activation du suivi avec la console Lambda

Pour activer le suivi actif de votre fonction d'événement Lambda à l'aide de la console, procédez comme suit :

Pour activer le traçage actif

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez une fonction d'événement.
3. Choisissez Configuration, puis choisissez Outils de surveillance et d’opérations.
4. Dans Outils de surveillance supplémentaires, choisissez Modifier.
5. Sous Signaux CloudWatch d'application et AWS X-Ray sélectionnez Activer les traces de service Lambda.
6. Cliquez sur Enregistrer.

Activation du suivi avec l'API Lambda

Configurez le suivi sur votre fonction Lambda avec le AWS SDK AWS CLI or, utilisez les opérations d'API suivantes :

- UpdateFunctionConfiguration
- GetFunctionConfiguration
- CreateFunction

L'exemple de AWS CLI commande suivant active le suivi actif sur une fonction nommée my-function.

```
aws lambda update-function-configuration --function-name my-function \
--tracing-config Mode=Active
```

Le mode de suivi fait partie de la configuration spécifique de la version lorsque vous publiez une version de votre fonction. Vous ne pouvez pas modifier le mode de suivi sur une version publiée.

Activation du traçage avec CloudFormation

Pour activer le suivi d'une `AWS::Lambda::Function` ressource dans un CloudFormation modèle, utilisez la `TracingConfig` propriété.

Example fonction-inline.yml — Configuration du suivi

```
Resources:
  function:
    Type: AWS::Lambda::Function
    Properties:
      TracingConfig:
        Mode: Active
      ...
```

Pour une `AWS::Serverless::Function` ressource AWS Serverless Application Model (AWS SAM), utilisez la `Tracing` propriété.

Example template.yml — Configuration du suivi

```
Resources:
  function:
```

```
    Type: AWS::Serverless::Function
    Properties:
      Tracing: Active
      ...
```

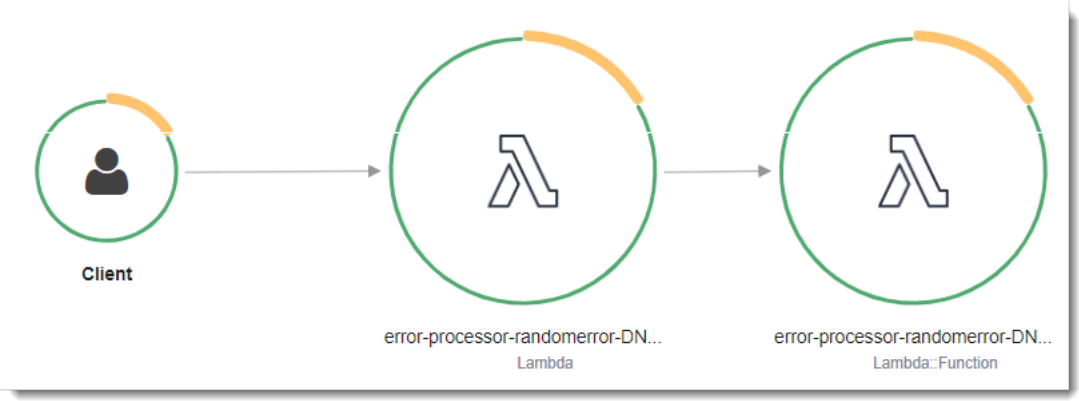
Interprétation et X-Ray traçage

Votre fonction événementielle a besoin d'une autorisation pour télécharger des données de suivi sur X-Ray. Lorsque vous activez le suivi dans la console Lambda, Lambda ajoute les autorisations requises au rôle d'exécution de votre fonction d'événement. Dans le cas contraire, ajoutez la AWSXRayDaemonWriteAccesspolitique au rôle d'exécution.

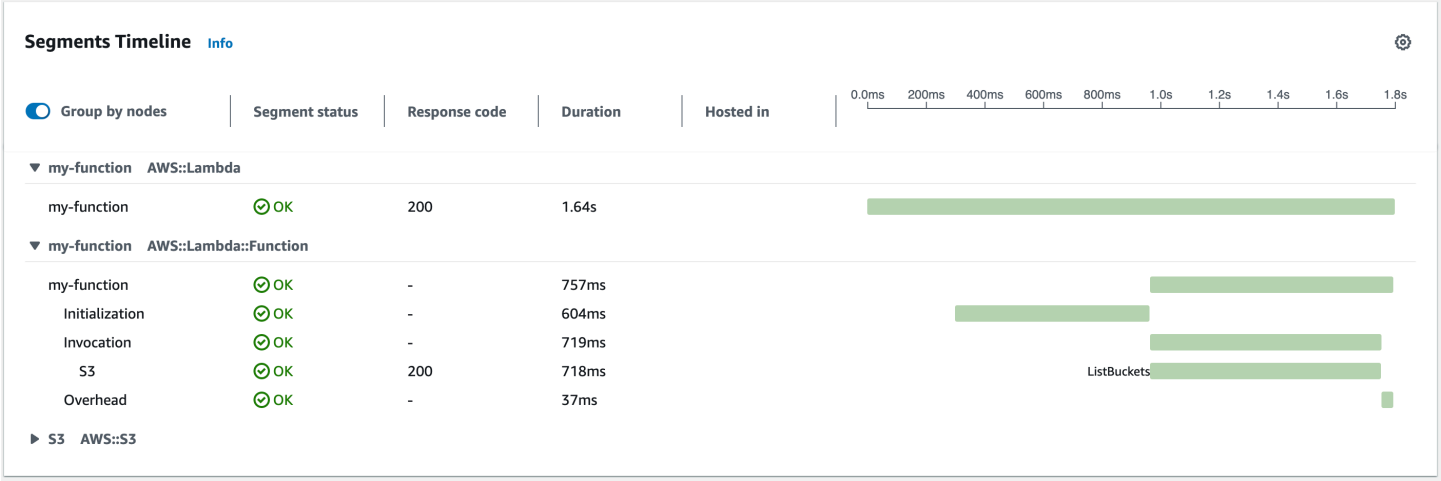
Une fois que vous avez configuré le suivi actif, vous pouvez observer des demandes spécifiques via votre application. Le graphique X-Ray de service affiche des informations sur votre application et tous ses composants. L'exemple suivant montre une application dotée de deux fonctions. La fonction principale traite les événements et renvoie parfois des erreurs. La deuxième fonction située en haut traite les erreurs qui apparaissent dans le groupe de journaux de la première et utilise le AWS SDK pour appeler X-Ray Amazon Simple Storage Service (Amazon S3) et Amazon Logs. CloudWatch

X-Ray ne retrace pas toutes les demandes jusqu'à votre application. X-Ray applique un algorithme d'échantillonnage pour garantir l'efficacité du suivi, tout en fournissant un échantillon représentatif de toutes les demandes. Le taux d'échantillonnage est 1 demande par seconde et 5 % de demandes supplémentaires. Vous ne pouvez pas configurer le taux X-Ray d'échantillonnage pour vos fonctions.

Dans X-Ray, un suivi enregistre des informations relatives à une demande traitée par un ou plusieurs services. Lambda enregistre deux segments par suivi, ce qui a pour effet de créer deux nœuds sur le graphique du service. L'image suivante met en évidence ces deux nœuds :



Le premier nœud sur la gauche représente le service Lambda qui reçoit la demande d'invocation. Le deuxième nœud représente votre fonction Lambda spécifique. L'exemple suivant illustre une trace avec ces deux segments. Les deux sont nommés my-function, mais l'un a pour origine `AWS::Lambda` et l'autre a pour origine `AWS::Lambda::Function`. Si le segment `AWS::Lambda` affiche une erreur, cela signifie que le service Lambda a rencontré un problème. Si le segment `AWS::Lambda::Function` affiche une erreur, cela signifie que votre fonction a rencontré un problème.



Cet exemple développe le segment `AWS::Lambda::Function` pour afficher ses trois sous-segments.

> **Note**
>
> AWS met actuellement en œuvre des modifications du service Lambda. En raison de ces modifications, vous pouvez constater des différences mineures entre la structure et le contenu des messages du journal système et des segments de trace émis par les différentes fonctions d'événement Lambda de votre ordinateur. Compte AWS

L'exemple de suivi présenté ici illustre le segment de fonction à l'ancienne. Les différences entre les segments à l'ancienne et de style moderne sont décrites dans les paragraphes suivants.
Ces modifications seront mises en œuvre au cours des prochaines semaines, et toutes les fonctions, Régions AWS sauf en Chine et dans les GovCloud régions, seront transférées pour utiliser le nouveau format des messages de journal et des segments de trace.

Le segment de fonction à l'ancienne contient les sous-segments suivants :

- Initialization (Initialisation) : représente le temps passé à charger votre fonction et à exécuter le code d'initialisation. Ce sous-segment apparaît pour le premier événement traité par chaque instance de votre fonction.
- Invocation – Représente le temps passé à exécuter votre code de gestionnaire.
- Overhead (Travail supplémentaire) – Représente le temps que le fichier d'exécution Lambda passe à se préparer à gérer l'événement suivant.

Le segment de fonction de style moderne ne contient pas de sous-segment `Invocation`. À la place, les sous-segments du client sont directement rattachés au segment de fonction. Pour plus d'informations sur la structure des segments de fonction à l'ancienne et de style moderne, consultez the section called "Comprendre les X-Ray traces".

Vous pouvez également utiliser des clients HTTP, enregistrer des requêtes SQL et créer des sous-segments personnalisés avec des annotations et des métadonnées. Pour plus d'informations, consultez Kit SDK AWS X-Ray pour .NET dans le AWS X-Ray Guide du développeur.

Tarification

Vous pouvez utiliser le X-Ray suivi gratuitement chaque mois jusqu'à une certaine limite dans le cadre du niveau AWS gratuit. Au-delà de ce seuil, les X-Ray frais de stockage et de récupération des traces sont facturés. Pour en savoir plus, consultez Pricing AWS X-Ray (Tarification).

AWS Lambda Test de la fonction événementielle en C#

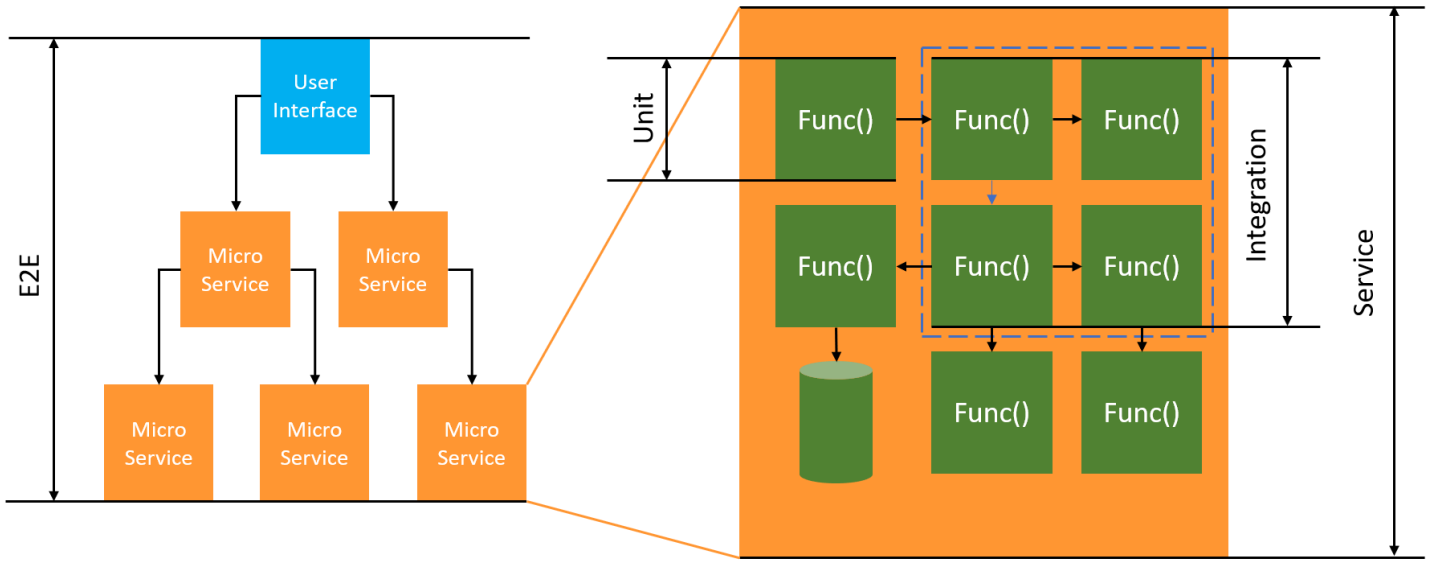
> **Note**
>
> Consultez le chapitre Test des fonctions pour une présentation complète des techniques et des bonnes pratiques pour tester les solutions sans serveur.

Le test des fonctions sans serveur utilise des types et des techniques de test traditionnels, mais vous devez également envisager de tester les applications sans serveur dans leur ensemble. Cloud-based les tests fournissent la mesure la plus précise de la qualité de vos fonctions et de vos applications sans serveur.

Une architecture d'application sans serveur comprend des services gérés qui fournissent des fonctionnalités d'applications critiques par le biais d'appels d'API. C'est pourquoi votre cycle de développement doit inclure des tests automatisés qui vérifient la fonctionnalité lorsque votre fonction et vos services interagissent.

Si vous ne créez pas de tests basés sur le cloud, vous pouvez rencontrer des problèmes en raison des différences entre votre environnement local et l'environnement déployé. Votre processus d'intégration continue doit exécuter des tests sur une série de ressources allouées dans le cloud avant de promouvoir votre code vers l'environnement de déploiement suivant, comme l'assurance qualité, la mise en place ou la production.

Poursuivez la lecture de ce petit guide pour en savoir plus sur les stratégies de test pour les applications sans serveur, ou rendez-vous sur le référentiel Serverless Test Samples pour vous plonger dans des exemples pratiques, spécifiques au langage et à l'exécution que vous avez choisis.



Pour les tests sans serveur, vous pouvez toujours écrire des tests unitaires, d'intégration et de bout en bout.

- Tests unitaires : tests exécutés sur un bloc de code isolé. Par exemple, la vérification de la logique métier permettant de calculer les frais de livraison en fonction d'un article et d'une destination donnés.
- Tests d'intégration : tests impliquant au moins deux composants ou services qui interagissent, généralement dans un environnement cloud. Par exemple, la vérification d'une fonction traite les événements d'une file d'attente.
- End-to-end tests - Tests qui vérifient le comportement dans l'ensemble d'une application. Il s'agit par exemple de s'assurer que l'infrastructure est correctement mise en place et que les événements circulent entre les services comme prévu pour enregistrer la commande d'un client.

Test de vos applications sans serveur

Vous utilisez généralement une combinaison d'approches pour tester le code de votre application sans serveur, notamment des tests dans le cloud, des tests avec des simulations et parfois des tests avec des émulateurs.

Tests dans le cloud

Les tests dans le cloud sont utiles pour toutes les phases des tests, y compris les tests unitaires, les tests d'intégration et les tests de bout en bout. Vous exécutez des tests sur du code déployé dans le cloud et interagissez avec des services basés sur le cloud. Cette approche fournit la mesure la plus précise de la qualité de votre code.

Un moyen pratique de déboguer votre fonction d'événement Lambda dans le cloud consiste à utiliser la console avec un événement de test. Un événement de test est une entrée JSON pour votre fonction. Si votre fonction ne nécessite pas d'entrée, l'événement peut être un document JSON vide (`{}`). La console fournit des exemples d'événements pour diverses intégrations de services. Après avoir créé un événement dans la console, vous pouvez le partager avec votre équipe pour faciliter les tests et les rendre plus cohérents.

> **Note**
>
> Tester une fonction dans la console est un moyen rapide de démarrer, mais l'automatisation de vos cycles de test garantit la qualité des applications et la rapidité du développement.

Outils de test

Pour accélérer votre cycle de développement, il existe un certain nombre d'outils et de techniques que vous pouvez utiliser pour tester vos fonctions. Par exemple, Accélérer AWS SAM et le mode de surveillance AWS CDK réduisent tous deux le temps nécessaire pour mettre à jour les environnements cloud.

La façon dont vous définissez votre code de fonction Lambda facilite l'ajout de tests d'unité. Lambda nécessite un constructeur public sans paramètre pour initialiser votre catégorie. L'introduction d'un deuxième constructeur interne vous permet de contrôler les dépendances utilisées par votre application.

```
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSerializer

namespace GetProductHandler;

public class Function
{
    private readonly IDatabaseRepository _repo;

    public Function(): this(null)
    {
    }

    internal Function(IDatabaseRepository repo)
    {
        this._repo = repo ?? new DatabaseRepository();
```

```
    }

    public async Task<APIGatewayProxyResponse> FunctionHandler(APIGatewayProxyRequest
 request)
    {
        var id = request.PathParameters["id"];

        var databaseRecord = await this._repo.GetById(id);

        return new APIGatewayProxyResponse
        {
            StatusCode = (int)HttpStatusCode.OK,
            Body = JsonSerializer.Serialize(databaseRecord)
        };
    }
}
```

Pour écrire un test pour cette fonction, vous pouvez initialiser une nouvelle instance de votre catégorie `Function` et transmettre une implémentation simulée du `IDatabaseRepository`. Les exemples ci-dessous utilisent `XUnit`, `Moq`, et `FluentAssertions` pour écrire un test simple permettant de s'assurer que le `FunctionHandler` renvoie un code d'état 200.

```
using Xunit;
using Moq;
using FluentAssertions;

public class FunctionTests
{
    [Fact]
    public async Task TestLambdaHandler_WhenInputIsValid_ShouldReturn200StatusCode()
    {
        // Arrange
        var mockDatabaseRepository = new Mock<IDatabaseRepository>();

        var functionUnderTest = new Function(mockDatabaseRepository.Object);

        // Act
        var response = await functionUnderTest.FunctionHandler(new
 APIGatewayProxyRequest());

        // Assert
        response.StatusCode.Should().Be(200);
    }
```

```
}
```

Pour des exemples plus détaillés, notamment des exemples de tests asynchrones, consultez le référentiel d'échantillons de tests .NET sur. GitHub

Création de fonctions d'événement Lambda avec PowerShell

Les sections suivantes expliquent comment les modèles de programmation courants et les concepts de base s'appliquent lorsque vous créez du code Lambda Event Function dans. PowerShell

Pour plus d'informations sur l'objet de PowerShell contexte, consultezthe section called “Contexte”.

Lambda fournit les exemples d'applications suivants pour : PowerShell

- blank-powershell — PowerShell Fonction qui montre l'utilisation de la journalisation, des variables d'environnement et du SDK. AWS

Avant de commencer, vous devez d'abord configurer un environnement PowerShell de développement. Pour obtenir des instructions sur la façon de procéder, veuillez consulter Configuration d'un environnement PowerShell de développement.

Pour savoir comment utiliser le AWSLambdaPSCore module pour télécharger des exemples de PowerShell projets à partir de modèles, créer des packages de PowerShell déploiement et déployer PowerShell des fonctions AWS dans le cloud, consultezDéployez les fonctions d'événement PowerShell Lambda avec des archives de fichiers .zip.

Lambda fournit les exécutions suivantes pour les langages .NET :

Nom	Identifiant	Système d’exploitation	Date d’obsolescence	Créer la fonction de blocage	Mettre à jour la fonction de blocage
.NET 10	`dotnet10`	Amazon Linux 2	14 novembre 2028	14 déc. 2028	15 janvier 2029
.NET 9 (conteneur uniquement)	`dotnet9`	Amazon Linux 2	10 novembre 2026	Non planifié	Non planifié

Nom	Identifiant	Système d'exploitation	Date d'obsolescence	Créer la fonction de blocage	Mettre à jour la fonction de blocage
.NET 8	`dotnet8`	Amazon Linux 2	10 novembre 2026	29 juillet 2027	31 août 2027

Rubriques

- Configuration d'un environnement PowerShell de développement
- Déployez les fonctions d'événement PowerShell Lambda avec des archives de fichiers .zip
- Définissez le gestionnaire de fonctions d'événement Lambda dans PowerShell
- Utilisation de l'objet de contexte Lambda pour récupérer les informations de la fonction PowerShell d'événement
- Enregistrez et surveillez les fonctions d'événements Powershell Lambda

Configuration d'un environnement PowerShell de développement

Lambda fournit un ensemble d'outils et de bibliothèques pour le PowerShell runtime. Pour les instructions d'installation, reportez-vous à la section Outils Lambda pour PowerShell activer. GitHub

Le AWSLambdaPSCore module inclut les applets de commande suivants pour aider à créer et à publier des fonctions d'événement PowerShell Lambda :

- Get-AWSPowerShellLambdaTemplate— Renvoie la liste des modèles de démarrage.
- New-AWSPowerShellLambda— Crée un PowerShell script initial basé sur un modèle.
- Publish-AWSPowerShellLambda— Publie un PowerShell script donné sur Lambda.
- New-AWSPowerShellLambdaPackage— Crée un package de déploiement Lambda que vous pouvez utiliser dans un CI/CD système pour le déploiement.

Déployez les fonctions d'événement PowerShell Lambda avec des archives de fichiers .zip

Un package de déploiement pour l' PowerShell environnement d'exécution contient votre PowerShell script, les PowerShell modules requis pour votre PowerShell script et les assemblys nécessaires pour héberger PowerShell Core.

Création de la fonction d'événement Lambda

Pour commencer à écrire et à invoquer un PowerShell script avec Lambda, vous pouvez utiliser `New-AWSPowerShellLambda` l'applet de commande pour créer un script de démarrage basé sur un modèle. Vous pouvez utiliser la cmdlet `Publish-AWSPowerShellLambda` pour déployer votre script vers Lambda. Ensuite, vous pouvez tester votre script via la ligne de commande ou la console Lambda.

Pour créer un nouveau PowerShell script, le télécharger et le tester, procédez comme suit :

1. Pour afficher la liste des modèles disponibles, exécutez la commande suivante :

   ```
   PS C:\> Get-AWSPowerShellLambdaTemplate

   Template               Description
   --------               -----------
   Basic                  Bare bones script
   CodeCommitTrigger      Script to process AWS CodeCommit Triggers
   ...
   ```

2. Pour créer un exemple de script basé sur le modèle `Basic`, exécutez la commande suivante :

   ```
   New-AWSPowerShellLambda -ScriptName MyFirstPSScript -Template Basic
   ```

   Un nouveau fichier nommé `MyFirstPSScript.ps1` est créé dans un nouveau sous-répertoire du répertoire actuel. Le nom de ce répertoire est basé sur le paramètre `-ScriptName`. Vous pouvez utiliser le paramètre `-Directory` pour choisir un autre répertoire.

   Vous pouvez voir que le nouveau fichier a le contenu suivant :

   ```
   # PowerShell script file to run as a Lambda function
   #
   # When executing in Lambda the following variables are predefined.
   ```

```
#   $LambdaInput - A PSObject that contains the Lambda function input data.
#   $LambdaContext - An Amazon.Lambda.Core.ILambdaContext object that contains
 information about the currently running Lambda environment.
#
# The last item in the PowerShell pipeline is returned as the result of the Lambda
 function.
#
# To include PowerShell modules with your Lambda function, like the
 AWSPowerShell.NetCore module, add a "#Requires" statement
# indicating the module and version.

#Requires -Modules @{ModuleName='AWSPowerShell.NetCore';ModuleVersion='3.3.618.0'}

# Uncomment to send the input to CloudWatch Logs
# Write-Host (ConvertTo-Json -InputObject $LambdaInput -Compress -Depth 5)
```

3. Pour savoir comment les messages de journal de votre PowerShell script sont envoyés à Amazon CloudWatch Logs, décommentez la `Write-Host` ligne de l'exemple de script.

   Pour illustrer comment renvoyer des données à partir de vos fonctions Lambda, ajoutez une ligne à la fin du script avec `$PSVersionTable`. Cela ajoute le `$PSVersionTable` au PowerShell pipeline. Une fois le PowerShell script terminé, le dernier objet du PowerShell pipeline correspond aux données renvoyées par la fonction Lambda. `$PSVersionTable`est une variable PowerShell globale qui fournit également des informations sur l'environnement d'exécution.

   Après avoir effectué ces modifications, les deux dernières lignes de l'exemple de script ressemblent à ce qui suit :

   ```
   Write-Host (ConvertTo-Json -InputObject $LambdaInput -Compress -Depth 5)
   $PSVersionTable
   ```

4. Après avoir modifié le fichier `MyFirstPSScript.ps1`, modifiez le répertoire en spécifiant l'emplacement du script. Exécutez ensuite la commande suivante pour publier le script dans Lambda :

   ```
   Publish-AWSPowerShellLambda -ScriptPath .\MyFirstPSScript.ps1 -Name
    MyFirstPSScript -Region us-east-2
   ```

   Notez que le paramètre `-Name` spécifie le nom de la fonction Lambda qui s'affiche dans la console Lambda. Vous pouvez utiliser cette fonction pour appeler manuellement votre script.

5. Appelez votre fonction à l'aide de la `invoke` commande AWS Command Line Interface (AWS CLI).

```
> aws lambda invoke --function-name MyFirstPSScript out
```

Définissez le gestionnaire de fonctions d'événement Lambda dans PowerShell

Lorsqu'une fonction Lambda est invoquée, le gestionnaire Lambda appelle le script. PowerShell

Lorsque le PowerShell script est invoqué, les variables suivantes sont prédéfinies :

- *$LambdaInput*— Un PSObject qui contient l'entrée du gestionnaire. Ces données d'entrée peuvent être des données d'événement (publiées par une source d'événement) ou des données d'entrée personnalisées que vous fournissez, telles qu'une chaîne ou n'importe quel objet de données personnalisé.
- *$LambdaContext*— Amazon.Lambda.Core.ILambdaContext Objet que vous pouvez utiliser pour accéder aux informations relatives à l'appel en cours, telles que le nom de la fonction en cours, la limite de mémoire, le temps d'exécution restant et la journalisation.

Par exemple, considérez l' PowerShell exemple de code suivant.

```
#Requires -Modules @{ModuleName='AWSPowerShell.NetCore';ModuleVersion='3.3.618.0'}
Write-Host 'Function Name:' $LambdaContext.FunctionName
```

Ce script renvoie la FunctionName propriété obtenue à partir de la LambdaContext variable $.

> **Note**
>
> Vous devez utiliser l'`#Requires`instruction dans vos PowerShell scripts pour indiquer les modules dont dépendent vos scripts. Cette instruction effectue deux tâches importantes. 1) Il communique aux autres développeurs les modules utilisés par le script, et 2) il identifie les modules dépendants que les AWS PowerShell outils doivent intégrer au script, dans le cadre du déploiement. Pour plus d'informations sur l'`#Requires`instruction dans PowerShell, voir À propos des exigences. Pour plus d'informations sur les packages de PowerShell déploiement, consultezDéployez les fonctions d'événement PowerShell Lambda avec des archives de fichiers .zip.
>
> Lorsque votre fonction PowerShell Lambda utilise les AWS PowerShell applets de commande, veillez à définir une `#Requires` instruction qui fait référence au module, qui prend en charge PowerShell Core, et non au `AWSPowerShell.NetCore` module, qui ne prend en charge que `AWSPowerShell` Windows. PowerShell De plus, veillez à utiliser la version 3.3.270.0 ou plus récente de `AWSPowerShell.NetCore`, qui optimise le processus d'importation d'applet de commande. Si vous utilisez une version plus ancienne, vous

connaîtrez des démarrages à froid plus longs. Pour plus d'informations, consultez AWS Outils pour PowerShell.

Renvoi de données

Certains appels Lambda sont destinés à renvoyer des données à leur appelant. Par exemple, si un appel répond à une demande web provenant d'API Gateway, notre fonction Lambda doit renvoyer la réponse. Pour PowerShell Lambda, le dernier objet ajouté au PowerShell pipeline est constitué des données renvoyées par l'invocation Lambda. Si l'objet est une chaîne, les données sont renvoyées en l'état. Dans le cas contraire, l'objet est converti en données JSON à l'aide de l'applet de commande `ConvertTo-Json`.

Par exemple, considérez l' PowerShell instruction suivante, qui `$PSVersionTable` s'ajoute au PowerShell pipeline :

```
$PSVersionTable
```

Une fois le PowerShell script terminé, le dernier objet du PowerShell pipeline correspond aux données renvoyées par la fonction Lambda. `$PSVersionTable`est une variable PowerShell globale qui fournit également des informations sur l'environnement d'exécution.

Utilisation de l'objet de contexte Lambda pour récupérer les informations de la fonction PowerShell d'événement

Lorsque Lambda exécute votre fonction, il transmet les informations de contexte en mettant une variable `$LambdaContext` à la disposition du gestionnaire. Cette variable fournit des méthodes et des propriétés avec des informations sur l'appel, la fonction et l'environnement d'exécution.

Propriétés du contexte

- `FunctionName` – Nom de la fonction Lambda.
- `FunctionVersion` – Version de la fonction.
- `InvokedFunctionArn` – Amazon Resource Name (ARN) utilisé pour appeler la fonction. Indique si l'appelant a spécifié un numéro de version ou un alias.
- `MemoryLimitInMB` – Quantité de mémoire allouée à la fonction.
- `AwsRequestId` – Identifiant de la demande d'invocation.
- `LogGroupName` – Groupe de journaux pour la fonction.
- `LogStreamName` – Flux de journal de l'instance de fonction.
- `RemainingTime` – Nombre de millisecondes restant avant l'expiration de l'exécution.
- `Identity` – (applications mobiles) Informations sur l'identité Amazon Cognito qui a autorisé la demande.
- `ClientContext` – (applications mobiles) Contexte client fourni à Lambda par l'application client.
- `Logger` – Objet enregistreur pour la fonction.

L'extrait de PowerShell code suivant montre une fonction de gestion simple qui imprime certaines informations contextuelles.

```
#Requires -Modules @{ModuleName='AWSPowerShell.NetCore';ModuleVersion='3.3.618.0'}
Write-Host 'Function name:' $LambdaContext.FunctionName
Write-Host 'Remaining milliseconds:' $LambdaContext.RemainingTime.TotalMilliseconds
Write-Host 'Log group name:' $LambdaContext.LogGroupName
Write-Host 'Log stream name:' $LambdaContext.LogStreamName
```

Enregistrez et surveillez les fonctions d'événements Powershell Lambda

AWS Lambda surveille automatiquement les fonctions d'événement Lambda en votre nom et envoie les journaux à Amazon. CloudWatch Votre fonction est fournie avec un groupe de CloudWatch journaux Logs et un flux de journaux pour chaque instance de votre fonction. L'environnement d'exécution Lambda envoie des informations sur chaque invocation au flux de journaux et transmet les journaux et autres sorties provenant du code de votre fonction. Pour plus d'informations, consultez Envoi des journaux des fonctions d'événements Lambda aux journaux CloudWatch.

Cette page explique comment générer une sortie de journal à partir du code de votre fonction Lambda et comment accéder aux journaux à l'aide de la AWS Command Line Interface console Lambda ou de la console. CloudWatch

Sections

- Création d'une fonction qui renvoie des journaux
- Affichage des journaux dans la console Lambda
- Afficher les journaux dans la CloudWatch console
- Afficher les journaux à l'aide du AWS Command Line Interface (AWS CLI)
- Suppression de journaux

Création d'une fonction qui renvoie des journaux

Pour générer des journaux à partir de votre code de fonction, vous pouvez utiliser des applets de commande activé Microsoft.PowerShell.Utilityou tout autre module de journalisation qui écrit dans ou. `stdout` `stderr` L'exemple suivant utilise `Write-Host`.

Example function/Handler.ps1 — Journalisation

```
#Requires -Modules @{ModuleName='AWSPowerShell.NetCore';ModuleVersion='3.3.618.0'}
Write-Host `## Environment variables
Write-Host AWS_LAMBDA_FUNCTION_VERSION=$Env:AWS_LAMBDA_FUNCTION_VERSION
Write-Host AWS_LAMBDA_LOG_GROUP_NAME=$Env:AWS_LAMBDA_LOG_GROUP_NAME
Write-Host AWS_LAMBDA_LOG_STREAM_NAME=$Env:AWS_LAMBDA_LOG_STREAM_NAME
Write-Host AWS_EXECUTION_ENV=$Env:AWS_EXECUTION_ENV
Write-Host AWS_LAMBDA_FUNCTION_NAME=$Env:AWS_LAMBDA_FUNCTION_NAME
Write-Host PATH=$Env:PATH
Write-Host `## Event
Write-Host (ConvertTo-Json -InputObject $LambdaInput -Compress -Depth 3)
```

Example format des journaux

```
START RequestId: 56639408-xmpl-435f-9041-ac47ae25ceed Version: $LATEST
Importing module ./Modules/AWSPowerShell.NetCore/3.3.618.0/AWSPowerShell.NetCore.psd1
[Information] - ## Environment variables
[Information] - AWS_LAMBDA_FUNCTION_VERSION=$LATEST
[Information] - AWS_LAMBDA_LOG_GROUP_NAME=/aws/lambda/blank-powershell-
function-18CIXMPLHFAJJ
[Information] - AWS_LAMBDA_LOG_STREAM_NAME=2020/04/01/
[$LATEST]53c5xmpl52d64ed3a744724d9c201089
[Information] - AWS_EXECUTION_ENV=AWS_Lambda_dotnet6_powershell_1.0.0
[Information] - AWS_LAMBDA_FUNCTION_NAME=blank-powershell-function-18CIXMPLHFAJJ
[Information] - PATH=/var/lang/bin:/usr/local/bin:/usr/bin/:/bin:/opt/bin
[Information] - ## Event
[Information] -
{
    "Records": [
        {
            "messageId": "19dd0b57-b21e-4ac1-bd88-01bbb068cb78",
            "receiptHandle": "MessageReceiptHandle",
            "body": "Hello from SQS!",
            "attributes": {
                "ApproximateReceiveCount": "1",
                "SentTimestamp": "1523232000000",
                "SenderId": "123456789012",
                "ApproximateFirstReceiveTimestamp": "1523232000001"
            },
            ...
END RequestId: 56639408-xmpl-435f-9041-ac47ae25ceed
REPORT RequestId: 56639408-xmpl-435f-9041-ac47ae25ceed Duration: 3906.38 ms Billed
 Duration: 9867 ms Memory Size: 512 MB Max Memory Used: 367 MB Init Duration: 5960.19
 ms
XRAY TraceId: 1-5e843da6-733cxmple7d0c3c020510040 SegmentId: 3913xmpl20999446 Sampled:
 true
```

L'environnement d'exécution .NET enregistre les lignes `START`, `END` et `REPORT` pour chaque invocation. La ligne de rapport fournit les détails suivants.

Champs de données de la ligne REPORT

- RequestId— L'identifiant de demande unique pour l'invocation.

- Duration – Temps que la méthode de gestion du gestionnaire de votre fonction a consacré au traitement de l'événement.
- Billed Duration : temps facturé pour l'invocation.
- Memory Size – Quantité de mémoire allouée à la fonction.
- Max Memory Used – Quantité de mémoire utilisée par la fonction. Lorsque les appels partagent un environnement d'exécution, Lambda indique la mémoire maximale utilisée pour toutes les invocations. Ce comportement peut entraîner une valeur signalée plus élevée que prévu.
- Init Duration : pour la première requête servie, temps qu'il a pris à l'exécution charger la fonction et exécuter le code en dehors de la méthode du gestionnaire.
- XRAY TraceId — Pour les demandes suivies, l'ID de AWS X-Ray trace.
- SegmentId— Pour les demandes suivies, l'ID X-Ray du segment.
- Sampled – Pour les demandes suivies, résultat de l'échantillonnage.

Affichage des journaux dans la console Lambda

Vous pouvez utiliser la console Lambda pour consulter les résultats du journal après avoir invoqué une fonction d'événement Lambda.

Si votre code peut être testé à partir de l'éditeur de code intégré, vous trouverez des journaux dans les résultats d'exécution. Lorsque vous utilisez la fonctionnalité de test de la console pour appeler une fonction, vous trouverez la sortie du journal dans la section Détails.

Afficher les journaux dans la CloudWatch console

Vous pouvez utiliser la CloudWatch console Amazon pour consulter les journaux de toutes les invocations de la fonction d'événement Lambda.

Pour afficher les journaux sur la CloudWatch console

1. Ouvrez la page Groupes de journaux sur la CloudWatch console.
2. Choisissez le groupe de journaux pour votre fonction (/aws/lambda/***your-function-name***).
3. Choisissez un flux de journaux.

Chaque flux de journal correspond à une instance de votre fonction. Un flux de journal apparaît lorsque vous mettez à jour votre fonction Lambda et lorsque des instances supplémentaires sont créées pour gérer les appels simultanés. Pour trouver les journaux d'un appel spécifique, nous vous

recommandons d'instrumenter votre fonction avec. AWS X-Ray X-Ray enregistre les détails de la demande et du flux de log dans le traçage.

Afficher les journaux à l'aide du AWS Command Line Interface (AWS CLI)

AWS CLI Il s'agit d'un outil open source que vous pouvez utiliser pour interagir avec les AWS services à l'aide de commandes dans votre interface de ligne de commande. Pour effectuer les étapes de cette section, vous devez disposer de la version 2 de l'AWS CLI.

Vous pouvez utiliser AWS CLI pour récupérer les journaux d'une invocation à l'aide de l'option de commande `--log-type`. La réponse inclut un champ `LogResult` qui contient jusqu'à 4 Ko de journaux codés en base64 provenant de l'invocation.

Example récupérer un ID de journal

L'exemple suivant montre comment récupérer un ID de journal à partir du champ `LogResult` d'une fonction nommée `my-function`.

```
aws lambda invoke --function-name my-function out --log-type Tail
```

Vous devriez voir la sortie suivante:

```
{
    "StatusCode": 200,
    "LogResult":
 "U1RBUlQgUmVxdWVzdElkOiA4N2QwNDRiOC1mMTU0LTExZTgtOGNkYS0yOTc0YzVlNGZiMjEgVmVyc2lvb...",
    "ExecutedVersion": "$LATEST"
}
```

Example décoder les journaux

Dans la même invite de commandes, utilisez l'utilitaire `base64` pour décoder les journaux. L'exemple suivant montre comment récupérer les journaux encodés en base64 pour `my-function`.

```
aws lambda invoke --function-name my-function out --log-type Tail \
--query 'LogResult' --output text --cli-binary-format raw-in-base64-out | base64 --
decode
```

L'cli-binary-formatoption est obligatoire si vous utilisez AWS CLI la version 2. Pour faire de ce paramètre le paramètre par défaut, exécutez `aws configure set cli-binary-format raw-`

`in-base64-out`. Pour plus d'informations, consultez les options de ligne de commande globales AWS CLI prises en charge dans le Guide de l'utilisateur AWS Command Line Interface version 2.

Vous devriez voir la sortie suivante :

```
START RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8 Version: $LATEST
"AWS_SESSION_TOKEN": "AgoJb3JpZ2luX2VjELj...", "_X_AMZN_TRACE_ID": "Root=1-5d02e5ca-
f5792818b6fe8368e5b51d50;Parent=191db58857df8395;Sampled=0"",ask/lib:/opt/lib",
END RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8
REPORT RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8  Duration: 79.67 ms      Billed
 Duration: 80 ms         Memory Size: 128 MB     Max Memory Used: 73 MB
```

L'utilitaire `base64` est disponible sous Linux, macOS et Ubuntu sous Windows. Les utilisateurs de macOS auront peut-être besoin d'utiliser `base64 -D`.

Example Script get-logs.sh

Dans la même invite de commandes, utilisez le script suivant pour télécharger les cinq derniers événements de journalisation. Le script utilise `sed` pour supprimer les guillemets du fichier de sortie et attend 15 secondes pour permettre la mise à disposition des journaux. La sortie comprend la réponse de Lambda, ainsi que la sortie de la commande `get-log-events`.

Copiez le contenu de l'exemple de code suivant et enregistrez-le dans votre répertoire de projet Lambda sous `get-logs.sh`.

L'cli-binary-formatoption est obligatoire si vous utilisez AWS CLI la version 2. Pour faire de ce paramètre le paramètre par défaut, exécutez `aws configure set cli-binary-format raw-in-base64-out`. Pour plus d'informations, consultez les options de ligne de commande globales AWS CLI prises en charge dans le Guide de l'utilisateur AWS Command Line Interface version 2.

```
#!/bin/bash
aws lambda invoke --function-name my-function --cli-binary-format raw-in-base64-out --
payload '{"key": "value"}' out
sed -i'' -e 's/"//g' out
sleep 15
aws logs get-log-events --log-group-name /aws/lambda/my-function --log-stream-
name stream1 --limit 5
```

Example macOS et Linux (uniquement)

Dans la même invite de commande, les utilisateurs de macOS et de Linux devront peut-être exécuter la commande suivante pour s'assurer que le script est exécutable.

```
chmod -R 755 get-logs.sh
```

Example récupérer les cinq derniers événements de journal

Dans la même invite de commande, exécutez le script suivant pour obtenir les cinq derniers événements de journalisation.

```
./get-logs.sh
```

Vous devriez voir la sortie suivante:

```
{
    "StatusCode": 200,
    "ExecutedVersion": "$LATEST"
}
{
    "events": [
        {
            "timestamp": 1559763003171,
            "message": "START RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf Version:
 $LATEST\n",
            "ingestionTime": 1559763003309
        },
        {
            "timestamp": 1559763003173,
            "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tENVIRONMENT VARIABLES\r{\r  \"AWS_LAMBDA_FUNCTION_VERSION\": \"$LATEST\",
\r ...",
            "ingestionTime": 1559763018353
        },
        {
            "timestamp": 1559763003173,
            "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tEVENT\r{\r  \"key\": \"value\"\r}\n",
            "ingestionTime": 1559763018353
        },
        {
            "timestamp": 1559763003218,
            "message": "END RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf\n",
            "ingestionTime": 1559763018353
        },
        {
```

```
            "timestamp": 1559763003218,
            "message": "REPORT RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tDuration: 26.73 ms\tBilled Duration: 27 ms \tMemory Size: 128 MB\tMax Memory Used: 75
 MB\t\n",
            "ingestionTime": 1559763018353
        }
    ],
    "nextForwardToken": "f/34783877304859518393868359594929986069206639495374241795",
    "nextBackwardToken": "b/34783877303811383369537420289090800615709599058929582080"
}
```

Suppression de journaux

Les groupes de journaux ne sont pas supprimés automatiquement quand vous supprimez une fonction. Pour éviter de stocker des journaux indéfiniment, supprimez le groupe de journaux ou configurez une période de conservation à l'issue de laquelle les journaux sont supprimés automatiquement.

Création de fonctions d'événements Lambda avec Rust

Comme Rust compile en code natif, vous n'avez pas besoin d'un environnement d'exécution dédié pour exécuter le code Rust en tant que fonction d'événement Lambda. Utilisez plutôt le client d'exécution Rust pour créer votre projet localement, puis déployez-le sur Lambda à l'aide d'un OS-only environnement d'exécution. Lorsque vous utilisez un OS-only environnement d'exécution, Lambda met automatiquement le système d'exploitation à jour avec les derniers correctifs. Pour plus d'informations sur l'utilisation des événements HTTP, consultezthe section called “Événements HTTP”. Pour plus d'informations sur l'utilisation de couches avec Rust, consultezthe section called “Layers”.

Outils et bibliothèques pour Rust

- AWS SDK pour Rust: Le AWS SDK pour Rust fournit des API Rust pour interagir avec les services d'infrastructure Amazon Web Services.
- Client d'exécution Rust pour Lambda : Le client d'exécution Rust facilite l'exécution de fonctions Lambda écrites en Rust.
- Cargo Lambda : il s'agit d'une extension open source tierce de l'outil de ligne de commande Cargo qui simplifie la création et le déploiement des fonctions Rust Lambda.
- Lambda HTTP : cette bibliothèque fournit un wrapper pour travailler avec des événements HTTP.

- Extension Lambda : cette bibliothèque fournit un support pour écrire des extensions Lambda avec Rust.
- AWS Lambda Événements : cette bibliothèque fournit des définitions de type pour les intégrations de sources d'événements courantes.

Exemples d’applications Lambda pour Rust

- Fonction Lambda de base : une fonction Rust qui montre comment traiter des événements de base.
- Fonction Lambda avec gestion des erreurs : une fonction Rust qui montre comment gérer des erreurs Rust personnalisées dans Lambda.
- Fonction Lambda avec ressources partagées : un projet Rust qui initialise les ressources partagées avant de créer la fonction Lambda.
- Événements HTTP Lambda : une fonction Rust qui gère les événements HTTP.
- Événements HTTP Lambda avec en-têtes CORS : une fonction Rust qui utilise Tower pour injecter des en-têtes CORS.
- API REST Lambda : une API REST qui utilise Axum et Diesel pour la connexion à une base de données PostgreSQL.
- Démo Rust sans serveur : un projet Rust qui montre l'utilisation des bibliothèques Rust de Lambda, de la journalisation, des variables d'environnement et du AWS SDK.
- Extension Lambda de base : une extension Rust qui montre comment traiter les événements d’extension de base.
- Extension Lambda Logs Amazon Data Firehose : une extension Rust qui montre comment envoyer les journaux Lambda à Firehose.

Rubriques

- Définir les gestionnaires de fonctions d'événement Lambda dans Rust
- Utilisation de l'objet de contexte Lambda pour récupérer les informations de la fonction d'événement Rust
- Traitement des événements HTTP avec Rust
- Déployez les fonctions événementielles Rust Lambda avec des archives de fichiers .zip
- Utilisation de couches pour les fonctions d'événements Rust Lambda
- Enregistrez et surveillez les fonctions des événements Rust Lambda

Définir les gestionnaires de fonctions d'événement Lambda dans Rust

Le gestionnaire de fonctions d'événement Lambda est la méthode de votre code de fonction qui traite les événements. Lorsque votre fonction est invoquée, Lambda exécute la méthode du gestionnaire. Votre fonction s'exécute jusqu'à ce que le gestionnaire renvoie une réponse, se ferme ou expire.

Cette page décrit comment utiliser les gestionnaires de fonctions d'événement Lambda dans Rust, y compris l'initialisation du projet, les conventions de dénomination et les meilleures pratiques. Cette page inclut également un exemple de fonction Lambda Rust qui collecte des informations relatives à une commande, produit un reçu sous forme de fichier texte et place ce fichier dans un compartiment Amazon Simple Storage Service (S3). Pour plus d'informations sur le déploiement de votre fonction après l'avoir écrite, consultez the section called "Déploiement d'archives de fichiers .zip".

Rubriques

- Configuration de votre projet de gestionnaire Rust
- Exemple de code de fonction d'événement Rust Lambda
- Définitions de classe valides pour les gestionnaires Rust
- Convention de nommage du gestionnaire
- Définition et accès à l'objet d'événement d'entrée
- Accès et utilisation de l'objet de contexte Lambda
- Utilisation de AWS SDK pour Rust dans votre gestionnaire
- Accès aux variables d'environnement
- Utilisation de l'état partagé
- Bonnes pratiques en matière de code pour les fonctions d'événements Rust Lambda

Configuration de votre projet de gestionnaire Rust

Lorsque vous travaillez avec les fonctions d'événement Lambda dans Rust, le processus consiste à écrire votre code, à le compiler et à déployer les artefacts compilés sur Lambda. Le moyen le plus simple de configurer un projet de gestionnaire Lambda dans Rust est d'utiliser l'environnement d'exécution AWS Lambda pour Rust. Malgré son nom, le AWS Lambda Runtime for Rust n'est pas un environnement d'exécution géré au même sens que dans Lambda pour Python, Java ou. Node.js Au lieu de cela, le AWS Lambda Runtime for Rust est un crate (`lambda_runtime`) qui permet d'écrire des fonctions Lambda dans Rust et de s'interfacer avec l'environnement d'exécution AWS Lambda de Rust.

Utilisez la commande suivante pour installer Cargo Lambda, une extension open source tierce de l'outil de ligne de commande Cargo qui simplifie la création et le déploiement des fonctions Rust Lambda :

```
cargo install cargo-lambda
```

Après avoir installé `cargo-lambda`, utilisez la commande suivante pour initialiser un nouveau projet de gestionnaire de fonction Lambda :

```
cargo lambda new example-rust
```

Lorsque vous exécutez cette commande, l'interface de ligne de commande (CLI) vous pose quelques questions concernant votre fonction Lambda :

- Fonction HTTP — Si vous avez l'intention d'appeler votre fonction via API Gateway ou une URL de fonction, répondez Oui. Dans le cas contraire, répondez Non. Dans l'exemple de code de cette page, nous invoquons notre fonction avec un événement JSON personnalisé. Nous répondons donc Non.
- Type d'événement : si vous avez l'intention d'utiliser une forme d'événement prédéfinie pour invoquer votre fonction, sélectionnez le type d'événement attendu approprié. Sinon, laissez cette option vide. Dans l'exemple de code de cette page, nous invoquons notre fonction avec un événement JSON personnalisé. Nous laissons donc cette option vide.

Une fois la commande exécutée avec succès, entrez dans le répertoire principal de votre projet :

```
cd example-rust
```

Cette commande génère un fichier `generic_handler.rs` et un fichier `main.rs` dans le répertoire `src`. `generic_handler.rs` peut être utilisé pour personnaliser un gestionnaire d'événements générique. Le fichier `main.rs` contient la logique de votre application principale. Le fichier `Cargo.toml` contient des métadonnées relatives à votre package et répertorie ses dépendances externes.

Exemple de code de fonction d'événement Rust Lambda

L'exemple de code de fonction Lambda Rust suivant prend en compte les informations relatives à une commande, produit un reçu sous forme de fichier texte et place ce fichier dans un compartiment Amazon S3.

Example Fonction d'événement **`Lambda main.rs`**

```
use aws_sdk_s3::{Client, primitives::ByteStream};
use lambda_runtime::{run, service_fn, Error, LambdaEvent};
use serde::{Deserialize, Serialize};
use serde_json::Value;
use std::env;

#[derive(Deserialize, Serialize)]
struct Order {
    order_id: String,
    amount: f64,
    item: String,
}

async fn function_handler(event: LambdaEvent<Value>) -> Result<String, Error> {
    let payload = event.payload;

    // Deserialize the incoming event into Order struct
    let order: Order = serde_json::from_value(payload)?;

    let bucket_name = env::var("RECEIPT_BUCKET")
        .map_err(|_| "RECEIPT_BUCKET environment variable is not set")?;

    let receipt_content = format!(
        "OrderID: {}\nAmount: ${:.2}\nItem: {}",
        order.order_id, order.amount, order.item
    );
    let key = format!("receipts/{}.txt", order.order_id);

    let config =
 aws_config::load_defaults(aws_config::BehaviorVersion::latest()).await;
    let s3_client = Client::new(&config);

    upload_receipt_to_s3(&s3_client, &bucket_name, &key, &receipt_content).await?;

    Ok("Success".to_string())
}

async fn upload_receipt_to_s3(
    client: &Client,
    bucket_name: &str,
    key: &str,
    content: &str,
```

```
) -> Result<(), Error> {
    client
        .put_object()
        .bucket(bucket_name)
        .key(key)
        .body(ByteStream::from(content.as_bytes().to_vec()))  // Fixed conversion
        .content_type("text/plain")
        .send()
        .await?;

    Ok(())
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    run(service_fn(function_handler)).await
}
```

Ce fichier `main.rs` comprend les sections suivantes :

- Instructions `use` : utilisez-les pour importer des conteneurs (crates) et méthodes Rust que votre fonction Lambda requiert.
- `#[derive(Deserialize, Serialize)]` : définissez la forme de l'événement d'entrée attendu dans cette structure Rust.
- `async fn function_handler(event: LambdaEvent<Value>) -> Result<String, Error>` : il s'agit de la méthode de gestion principale, qui contient la logique principale de votre application.
- `async fn upload_receipt_to_s3 (...)` : il s'agit d'une méthode auxiliaire référencée par la méthode `function_handler` principale.
- `#[tokio::main]` : il s'agit d'une macro qui marque le point d'entrée d'un programme Rust. Elle met également en place un environnement d'exécution Tokio, qui permet à votre méthode `main()` d'utiliser `async/await` et de s'exécuter de manière asynchrone.
- `async fn main() -> Result<(), Error>` : la fonction `main()` est le point d'entrée de votre code. À l'intérieur, nous spécifions `function_handler` comme méthode de gestionnaire principal.

Cargo.toml Fichier d'exemple

Le fichier `Cargo.toml` suivant accompagne cette fonction.

```
[package]
name = "example-rust"
version = "0.1.0"
edition = "2024"

[dependencies]
aws-config = "1.5.18"
aws-sdk-s3 = "1.78.0"
lambda_runtime = "0.13.0"
serde = { version = "1", features = ["derive"] }
serde_json = "1"
tokio = { version = "1", features = ["full"] }
```

Pour que cette fonction fonctionne correctement, son rôle d'exécution doit autoriser l'action `s3:PutObject`. Assurez-vous également de définir la variable d'environnement `RECEIPT_BUCKET`. Après une invocation réussie, le compartiment Amazon S3 doit contenir un fichier de reçu.

Définitions de classe valides pour les gestionnaires Rust

Dans la plupart des cas, les signatures du gestionnaire Lambda que vous définissez dans Rust ont le format suivant :

```
async fn function_handler(event: LambdaEvent<T>) -> Result<U, Error>
```

Pour ce gestionnaire :

- Le nom de ce gestionnaire est `function_handler`.
- L'entrée singulière du gestionnaire est un événement, et est de type `LambdaEvent<T>`.
  - `LambdaEvent` est un wrapper qui vient du conteneur (crate) `lambda_runtime`. L'utilisation de ce wrapper vous donne accès à l'objet de contexte, qui inclut des Lambda-specific métadonnées telles que l'ID de demande de l'invocation.
  - T est le type d'événement désérialisé. Par exemple, cela peut être `serde_json::Value`, qui permet au gestionnaire d'accepter n'importe quelle entrée JSON générique. Il peut également s'agir d'un type comme `ApiGatewayProxyRequest` si votre fonction attend un type d'entrée spécifique et prédéfini.
- Le type de retour du gestionnaire est `Result<U, Error>`.
  - U est le type de sortie désérialisé. U doit implémenter la caractéristique `serde::Serialize` afin que Lambda puisse convertir la valeur de retour en JSON. Par exemple, U peut être un

type simple comme `String`, `serde_json::Value` ou une structure personnalisée tant qu'il implémente `Serialize`. Lorsque votre code atteint une instruction Ok(U), cela indique une exécution réussie et votre fonction renvoie une valeur de type U.

- Lorsque votre code rencontre une erreur (c'est-à-dire`Err(Error)`), votre fonction enregistre l'erreur dans Amazon CloudWatch et renvoie une réponse d'erreur de type`Error`.

Dans notre exemple, la signature du gestionnaire ressemble à ce qui suit :

```
async fn function_handler(event: LambdaEvent<Value>) -> Result<String, Error>
```

Les autres signatures de gestionnaire valides peuvent présenter les caractéristiques suivantes :

- Omission du wrapper `LambdaEvent` : si vous omettez `LambdaEvent`, vous perdez l'accès à l'objet de contexte Lambda dans votre fonction. Voici un exemple de ce type de signature :

  ```
  async fn handler(event: serde_json::Value) -> Result<String, Error>
  ```

- Utilisation du type d'unité comme entrée : pour Rust, vous pouvez utiliser le type d'unité pour représenter une entrée vide. Cela est couramment utilisé pour les fonctions avec des invocations périodiques et planifiées. Voici un exemple de ce type de signature :

  ```
  async fn handler(_: ()) -> Result<Value, Error>
  ```

Convention de nommage du gestionnaire

Les gestionnaires Lambda dans Rust n'ont pas de restrictions de dénomination strictes. Bien que vous puissiez utiliser n'importe quel nom pour votre gestionnaire, les noms de fonctions en Rust suivent généralement le format de casse `snake_case`.

Pour les applications plus petites, comme dans cet exemple, vous pouvez utiliser un seul fichier `main.rs` pour contenir l'ensemble de votre code. Pour les projets plus importants, `main.rs` doit contenir le point d'entrée de votre fonction, mais vous pouvez avoir des fichiers supplémentaires pour séparer votre code en modules logiques. Par exemple, vous pouvez avoir la structure de fichiers suivante :

```
/example-rust
### src/
```

```
#   ### main.rs        # Entry point
#   ### handler.rs     # Contains main handler
#   ### services.rs    # [Optional] Back-end service calls
#   ### models.rs      # [Optional] Data models
### Cargo.toml
```

Définition et accès à l'objet d'événement d'entrée

JSON est le format d'entrée le plus courant et le plus standard pour les fonctions d'événement Lambda. Dans cet exemple, la fonction exige une entrée similaire à l'exemple suivant :

```
{
    "order_id": "12345",
    "amount": 199.99,
    "item": "Wireless Headphones"
}
```

En Rust, vous pouvez définir la forme de l'événement d'entrée attendu dans une structure. Dans cet exemple, nous définissons la structure suivante pour représenter un `Order` :

```
#[derive(Deserialize, Serialize)]
struct Order {
    order_id: String,
    amount: f64,
    item: String,
}
```

Cette structure correspond à la forme d'entrée attendue. Dans cet exemple, la macro `#[derive(Deserialize, Serialize)]` génère automatiquement du code pour la sérialisation et la désérialisation. Cela signifie que nous pouvons désérialiser le type JSON d'entrée générique dans notre structure à l'aide de la méthode `serde_json::from_value()`. Ceci est illustré dans les premières lignes du gestionnaire :

```
async fn function_handler(event: LambdaEvent<Value>) -> Result<String, Error> {
    let payload = event.payload;

    // Deserialize the incoming event into Order struct
    let order: Order = serde_json::from_value(payload)?;
    ...
}
```

Vous pouvez ensuite accéder aux champs de l'objet. Par exemple, `order.order_id` récupère la valeur de `order_id` à partir de l'entrée d'origine.

Pre-defined types d'événements d'entrée

De nombreux types d'événements d'entrée prédéfinis sont disponibles dans le conteneur (crate) `aws_lambda_events`. Par exemple, si vous avez l'intention d'invoquer votre fonction avec API Gateway, y compris l'importation suivante :

```
use aws_lambda_events::event::apigw::ApiGatewayProxyRequest;
```

assurez-vous que votre gestionnaire principal utilise la signature suivante :

```
async fn handler(event: LambdaEvent<ApiGatewayProxyRequest>) -> Result<String, Error> {
    let body = event.payload.body.unwrap_or_default();
    ...
}
```

Reportez-vous au conteneur aws_lambda_events pour plus d'informations sur les autres types d'événements d'entrée prédéfinis.

Accès et utilisation de l'objet de contexte Lambda

L'objet de contexte Lambda contient des informations sur l'invocation, la fonction et l'environnement d'exécution. En Rust, le wrapper `LambdaEvent` inclut l'objet de contexte. Par exemple, vous pouvez utiliser l'objet de contexte pour récupérer l'ID de demande de l'invocation en cours à l'aide du code suivant :

```
async fn function_handler(event: LambdaEvent<Value>) -> Result<String, Error> {
    let request_id = event.context.request_id;
    ...
}
```

Pour plus d'informations sur la copie d'objets, consultez the section called "Contexte".

Utilisation de AWS SDK pour Rust dans votre gestionnaire

Vous utiliserez souvent les fonctions Lambda pour interagir avec d'autres AWS ressources ou pour les mettre à jour. Le moyen le plus simple d'interagir avec ces ressources est d'utiliser AWS SDK pour Rust.

Pour ajouter des dépendances du SDK à votre fonction, ajoutez-les dans votre fichier `Cargo.toml`. Nous vous recommandons de n'ajouter que les bibliothèques dont vous avez besoin pour votre fonction. Dans l'exemple de code précédent, nous avons utilisé `aws_sdk_s3::Client`. Dans le fichier `Cargo.toml`, vous pouvez ajouter cette dépendance en ajoutant la ligne suivante sous la section `[dependencies]` :

```
aws-sdk-s3 = "1.78.0"
```

> **Note**
>
> Il ne s'agit peut-être pas de la version la plus récente. Choisissez la version adéquate pour votre application.

Importez ensuite les dépendances directement dans votre code :

```
use aws_sdk_s3::{Client, primitives::ByteStream};
```

L'exemple de code initialise ensuite un client Amazon S3 comme suit :

```
let config = aws_config::load_defaults(aws_config::BehaviorVersion::latest()).await;
let s3_client = Client::new(&config);
```

Après avoir initialisé votre client SDK, vous pouvez l'utiliser pour interagir avec d'autres AWS services. L'exemple de code appelle l'API `PutObject` Amazon S3 dans la fonction d'assistance `upload_receipt_to_s3`.

Accès aux variables d'environnement

Dans le code de votre gestionnaire, vous pouvez référencer n'importe quelle variable d'environnement à l'aide de la méthode `env::var`. Dans cet exemple, nous référençons la variable d'environnement `RECEIPT_BUCKET` définie à l'aide de la ligne de code suivante :

```
let bucket_name = env::var("RECEIPT_BUCKET")
    .map_err(|_| "RECEIPT_BUCKET environment variable is not set")?;
```

Utilisation de l'état partagé

Vous pouvez déclarer des variables partagées indépendantes du code du gestionnaire de votre fonction Lambda. Ces variables peuvent vous aider à charger des informations d'état pendant le Phase d'initialisation, avant que votre fonction ne reçoive des événements. Par exemple, vous pouvez modifier le code de cette page pour utiliser l'état partagé lors de l'initialisation du client Amazon S3 en mettant à jour la fonction `main` et la signature du gestionnaire :

```
async fn function_handler(client: &Client, event: LambdaEvent<Value>) -> Result<String,
 Error> {
    ...
    upload_receipt_to_s3(client, &bucket_name, &key, &receipt_content).await?;
    ...
}

...

#[tokio::main]
async fn main() -> Result<(), Error> {
    let shared_config = aws_config::from_env().load().await;
    let client = Client::new(&shared_config);
    let shared_client = &client;
    lambda_runtime::run(service_fn(move |event: LambdaEvent<Request>| async move {
        handler(&shared_client, event).await
    }))
    .await
```

Bonnes pratiques en matière de code pour les fonctions d'événements Rust Lambda

Respectez les directives de la liste suivante pour utiliser les pratiques exemplaires de codage lors de la création de vos fonctions Lambda :

- Séparez le gestionnaire Lambda de votre logique principale. Cela facilite la création d'une fonction plus testable à l'unité.
- Réduisez la complexité de vos dépendances. Privilégiez les infrastructures plus simples qui se chargent rapidement au démarrage de l'environnement d'exécution.
- Réduisez la taille de votre package de déploiement selon ses besoins d'exécution. Cela réduit le temps nécessaire au téléchargement et au déballage de votre package de déploiement avant l'invocation.

Tirez parti de la réutilisation de l'environnement d'exécution pour améliorer les performances de votre fonction. Initialisez les clients SDK et les connexions à la base de données en dehors du gestionnaire de fonctions et mettez en cache les actifs statiques localement dans le répertoire `/tmp`. Les invocations ultérieures traitées par la même instance de votre fonction peuvent réutiliser ces ressources. Cela permet d'économiser des coûts, tout en réduisant le temps d'exécution de la fonction.

Pour éviter des éventuelles fuites de données entre les invocations, n'utilisez pas l'environnement d'exécution pour stocker des données utilisateur, des événements ou d'autres informations ayant un impact sur la sécurité. Si votre fonction repose sur un état réversible qui ne peut pas être stocké en mémoire dans le gestionnaire, envisagez de créer une fonction distincte ou des versions distinctes d'une fonction pour chaque utilisateur.

Utilisez une directive keep-alive pour maintenir les connexions persistantes. Lambda purge les connexions inactives au fil du temps. Si vous tentez de réutiliser une connexion inactive lorsque vous invoquez une fonction, cela entraîne une erreur de connexion. Pour maintenir votre connexion persistante, utilisez la directive Keep-alive associée à votre environnement d'exécution. Pour un exemple, voir Réutilisation des connexions avec Keep-Alive in Node.js.

Utilisez des variables d'environnement pour transmettre des paramètres opérationnels à votre fonction. Par exemple, si vous écrivez dans un compartiment Amazon S3 au lieu de coder en dur le nom du compartiment dans lequel vous écrivez, configurez le nom du compartiment comme variable d'environnement.

Évitez d'utiliser des invocations récursives dans votre fonction Lambda, lorsque la fonction s'invoque elle-même ou démarre un processus susceptible de l'invoquer à nouveau. Cela peut entraîner un volume involontaire d'invocations de fonction et des coûts accrus. Si vous constatez un volume involontaire d'invocations, définissez immédiatement la simultanéité réservée à la fonction sur `0` afin de limiter toutes les invocations de la fonction, pendant que vous mettez à jour le code.

N'utilisez pas d'API non publiques non documentées dans le code de votre fonction Lambda. Pour les AWS Lambda environnements d'exécution gérés, Lambda applique régulièrement des mises à jour fonctionnelles et de sécurité aux API internes de Lambda. Ces mises à jour internes de l'API peuvent être incompatibles avec les versions antérieures, entraînant des conséquences imprévues telles que des échecs d'invocation si votre fonction dépend de ces API non publiques. Consultez la Référence d'API pour obtenir la liste des API accessibles au public.

Écriture du code idempotent. L'écriture de code idempotent pour vos fonctions garantit ne gestion identique des événements dupliqués. Votre code doit valider correctement les événements

et gérer correctement les événements dupliqués. Pour de plus amples informations, veuillez consulterComment faire en sorte que ma fonction Lambda soit idempotente ?.

Utilisation de l'objet de contexte Lambda pour récupérer les informations de la fonction d'événement Rust

Lorsque Lambda exécute votre fonction d'événement, il ajoute un objet de contexte à LambdaEvent celui que le gestionnaire reçoit. Cet objet fournit les propriétés avec des informations sur l'appel, la fonction et l'environnement d'exécution.

Propriétés du contexte

- `request_id`: ID de AWS demande généré par le service Lambda.
- `deadline` : le délai d'exécution de l'invocation en cours en millisecondes.
- `invoked_function_arn` : l'Amazon Resource Name (ARN) de la fonction Lambda en cours d'invocation.
- `xray_trace_id`: ID de AWS X-Ray trace pour l'appel en cours.
- `client_content`: objet de contexte client envoyé par le SDK AWS mobile. Ce champ est vide sauf si la fonction est invoquée à l'aide d'un SDK AWS mobile.
- `identity` : l'identité Amazon Cognito qui a invoqué la fonction. Ce champ est vide sauf si la demande d'invocation des API Lambda a été effectuée à l'aide d'informations d'identification AWS émises par les groupes d'identités Amazon Cognito.
- `env_config` : la configuration de la fonction Lambda à partir des variables d'environnement locales. Cette propriété comprend des informations telles que le nom de la fonction, l'allocation de mémoire, la version et les flux de journaux.

Accès aux informations du contexte d'appel

Les fonctions Lambda ont accès aux métadonnées sur leur environnement et la demande d'appel. L'objet `LambaEvent` que votre gestionnaire de fonction reçoit comprend les métadonnées `context` :

```
use lambda_runtime::{service_fn, LambdaEvent, Error};
use serde_json::{json, Value};

async fn handler(event: LambdaEvent<Value>) -> Result<Value, Error> {
    let invoked_function_arn = event.context.invoked_function_arn;
    Ok(json!({ "message": format!("Hello, this is function
 {invoked_function_arn}!") }))
}

#[tokio::main]
```

```
async fn main() -> Result<(), Error> {
    lambda_runtime::run(service_fn(handler)).await
}
```

Traitement des événements HTTP avec Rust

Les API Amazon API Gateway, les Application Load Balancers et les URL de fonction Lambda peuvent envoyer des événements HTTP à Lambda. Vous pouvez utiliser la caisse aws_lambda_events de crates.io pour traiter les événements provenant de ces sources.

Example– Gestion de la demande de proxy API Gateway

Notez ce qui suit :

- `use aws_lambda_events::apigw::{ApiGatewayProxyRequest, ApiGatewayProxyResponse}` : la caisse aws_lambda_events inclut de nombreux événements Lambda. Pour réduire le temps de compilation, utilisez les drapeaux de fonction pour activer les événements dont vous avez besoin. Exemple: `aws_lambda_events = { version = "0.8.3", default-features = false, features = ["apigw"] }`.
- `use http::HeaderMap` : cette importation nécessite d'ajouter la caisse http à vos dépendances.

```
use aws_lambda_events::apigw::{ApiGatewayProxyRequest, ApiGatewayProxyResponse};
use http::HeaderMap;
use lambda_runtime::{service_fn, Error, LambdaEvent};

async fn handler(
    _event: LambdaEvent<ApiGatewayProxyRequest>,
) -> Result<ApiGatewayProxyResponse, Error> {
    let mut headers = HeaderMap::new();
    headers.insert("content-type", "text/html".parse().unwrap());
    let resp = ApiGatewayProxyResponse {
        status_code: 200,
        multi_value_headers: headers.clone(),
        is_base64_encoded: false,
        body: Some("Hello AWS Lambda HTTP request".into()),
        headers,
    };
    Ok(resp)
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    lambda_runtime::run(service_fn(handler)).await
}
```

Le client d'exécution Rust pour Lambda fournit également une abstraction de ces types d'événements que vous pouvez utiliser avec des types HTTP natifs, quel que soit le service qui envoie les événements. Le code suivant est équivalent à l'exemple précédent, et il fonctionne d'emblée avec les URL des fonctions Lambda, les Application Load Balancer et l'API Gateway.

> **Note**
>
> À la base, la caisse lambda_http utilise la caisse lambda_runtime. Vous n'avez pas besoin d'importer `lambda_runtime` séparément.

Example– Gestion des requêtes HTTP

```
use lambda_http::{service_fn, Error, IntoResponse, Request, RequestExt, Response};

async fn handler(event: Request) -> Result<impl IntoResponse, Error> {
    let resp = Response::builder()
        .status(200)
        .header("content-type", "text/html")
        .body("Hello AWS Lambda HTTP request")
        .map_err(Box::new)?;
    Ok(resp)
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    lambda_http::run(service_fn(handler)).await
}
```

Pour un autre exemple d'utilisation`lambda_http`, consultez l'exemple de code http-axum sur le AWS référentiel Labs. GitHub

Exemples d'événements HTTP Lambda pour Rust

- Événements HTTP Lambda : une fonction Rust qui gère les événements HTTP.
- Événements HTTP Lambda avec en-têtes CORS : une fonction Rust qui utilise Tower pour injecter des en-têtes CORS.
- Événements HTTP Lambda avec ressources partagées : une fonction Rust qui utilise des ressources partagées initialisées avant la création du gestionnaire de fonction.

Déployez les fonctions événementielles Rust Lambda avec des archives de fichiers .zip

Cette page décrit comment compiler votre fonction Rust Event, puis déployer le binaire compilé sur AWS Lambda en utilisant Cargo Lambda. Il montre également comment déployer le binaire compilé avec le AWS Command Line Interface et le AWS Serverless Application Model CLI.

Sections

- Conditions préalables
- Création de fonctions Rust sur macOS, Windows ou Linux
- Déploiement du binaire de la fonction Rust avec Cargo Lambda
- Invocation de votre fonction Rust avec Cargo Lambda

Conditions préalables

- Rust
- AWS CLI version 2

Création de fonctions Rust sur macOS, Windows ou Linux

Les étapes suivantes montrent comment créer le projet pour votre première fonction Lambda avec Rust et le compiler avec Cargo Lambda, une extension open source tierce de l'outil de ligne de commande Cargo qui simplifie la création et le déploiement des fonctions Rust Lambda.

1. Installer Cargo Lambda, une extension open source tierce de l'outil de ligne de commande Cargo qui simplifie la création et le déploiement des fonctions Rust Lambda :

   ```
   cargo install cargo-lambda
   ```

   Pour d'autres options d'installation, voir Installation dans la documentation de Cargo Lambda.
2. Créez la structure du package. Cette commande crée un code de fonction de base dans `src/main.rs`. Vous pouvez utiliser ce code pour le tester ou le remplacer par le vôtre.

   ```
   cargo lambda new my-function
   ```
3. À l'intérieur du répertoire racine du package, exécutez la sous-commande build pour compiler le code de votre fonction.

```
cargo lambda build --release
```

(Facultatif) Si vous souhaitez utiliser AWS Graviton sur Lambda, ajoutez le `--arm64` indicateur pour compiler votre code pour les processeurs ARM.

```
cargo lambda build --release --arm64
```

4. Avant de déployer votre fonction Rust, configurez AWS informations d'identification sur votre machine.

```
aws configure
```

Déploiement du binaire de la fonction Rust avec Cargo Lambda

Utilisez la sous-commande deploy pour déployer le binaire compilé vers Lambda. Cette commande crée un rôle d'exécution, puis la fonction Lambda. Pour spécifier un rôle d'exécution existant, utilisez l'indicateur --iam-role.

```
cargo lambda deploy my-function
```

Déploiement de votre binaire de fonction Rust avec le AWS CLI

Vous pouvez également déployer votre binaire avec AWS CLI.

1. Utilisez la sous-commande build pour créer le package de déploiement .zip.

```
cargo lambda build --release --output-format zip
```

2. Pour déployer le package .zip vers Lambda, exécutez la commande create-function.

   - Pour `--runtime`, spécifiez `provided.al2023`. Il s'agit d'un OS-only exécution. OS-only les environnements d'exécution sont utilisés pour déployer des fichiers binaires compilés et des environnements d'exécution personnalisés sur Lambda.
   - Pour `--role`, spécifiez l'ARN du rôle d'exécution.

```
aws lambda create-function \
     --function-name my-function \
```

```
    --runtime provided.al2023 \
    --role arn:aws:iam::111122223333:role/lambda-role \
    --handler rust.handler \
    --zip-file fileb://target/lambda/my-function/bootstrap.zip
```

Déploiement de votre binaire de fonction Rust avec le AWS SAM INTERFACE DE LIGNE DE COMMANDE (CLI)

Vous pouvez également déployer votre binaire avec AWS SAM CLI.

1. Créez un AWS SAM modèle avec la définition de la ressource et de la propriété. Pour `Runtime`, spécifiez `provided.al2023`. Il s'agit d'un OS-only exécution. OS-only les environnements d'exécution sont utilisés pour déployer des fichiers binaires compilés et des environnements d'exécution personnalisés sur Lambda.

   Pour plus d'informations sur le déploiement de fonctions Lambda à l'aide de AWS SAM, voir AWS::Serverless::Fonction dans le AWS Serverless Application Model Guide du développeur.

   Example Définition des ressources et des propriétés SAM pour un binaire Rust

   ```
   AWSTemplateFormatVersion: '2010-09-09'
   Transform: AWS::Serverless-2016-10-31
   Description: SAM template for Rust binaries
   Resources:
     RustFunction:
       Type: AWS::Serverless::Function
       Properties:
         CodeUri: target/lambda/my-function/
         Handler: rust.handler
         Runtime: provided.al2023
   Outputs:
     RustFunction:
       Description: "Lambda Function ARN"
       Value: !GetAtt RustFunction.Arn
   ```

2. Utilisez la sous-commande build pour compiler la fonction.

   ```
   cargo lambda build --release
   ```

3. Utilisez la commande sam deploy pour déployer la fonction vers Lambda.

```
sam deploy --guided
```

Pour plus d'informations sur la création de fonctions Rust avec le AWS SAM CLI, voir Création de fonctions Rust Lambda avec Cargo Lambda dans le AWS Serverless Application Model Guide du développeur.

Invocation de votre fonction Rust avec Cargo Lambda

Utilisez la sous-commande invoke pour tester votre fonction avec une charge utile.

```
cargo lambda invoke --remote --data-ascii '{"command": "Hello world"}' my-function
```

Invoquer votre fonction Rust avec le AWS CLI

Vous pouvez également utiliser le AWS CLI pour invoquer la fonction.

```
aws lambda invoke --function-name my-function --cli-binary-format raw-in-base64-out --
payload '{"command": "Hello world"}' /tmp/out.txt
```

Le cli-binary-format l'option est requise si vous utilisez AWS CLI version 2. Pour faire de ce paramètre le paramètre par défaut, exécutez `aws configure set cli-binary-format raw-in-base64-out`. Pour plus d'informations, consultez les options de ligne de commande globales prises en charge par l'AWS CLI dans le Guide de l'utilisateur AWS Command Line Interface version 2.

Utilisation de couches pour les fonctions d'événements Rust Lambda

Nous ne recommandons pas d'utiliser des couches pour gérer les dépendances des fonctions d'événement Lambda écrites en Rust. Cela est dû au fait que les fonctions Rust se compilent en un seul exécutable, que vous fournissez à Lambda lorsque vous déployez votre fonction. Cet exécutable contient votre code de fonction compilé, ainsi que toutes ses dépendances. L'utilisation de couches complique non seulement ce processus, mais entraîne également une augmentation des temps de démarrage à froid, car vos fonctions doivent charger manuellement des assemblages supplémentaires en mémoire pendant la phase d'initialisation.

Pour utiliser des dépendances externes avec vos gestionnaires Rust, incluez-les directement dans votre package de déploiement. Ce faisant, vous simplifiez le processus de déploiement et profitez des optimisations du compilateur Rust intégré. Pour un exemple d'importation et d'utilisation d'une dépendance telle que le kit SDK AWS pour Rust dans votre fonction, consultez the section called "Handler (Gestionnaire)".

Enregistrez et surveillez les fonctions des événements Rust Lambda

AWS Lambda surveille automatiquement les fonctions d'événement Lambda en votre nom et envoie les journaux à Amazon. CloudWatch Votre fonction Lambda est fournie avec un groupe de CloudWatch journaux Logs et un flux de journaux pour chaque instance de votre fonction. L'environnement d'exécution Lambda envoie des informations sur chaque invocation au flux de journaux et transmet les journaux et autres sorties provenant du code de votre fonction.

Pour plus d'informations, consultez Envoi des journaux des fonctions d'événements Lambda aux journaux CloudWatch. Pour plus d'informations sur la configuration des formats de journal, consultezConfiguration des formats de journal JSON et en texte brut. Cette page décrit comment produire des journaux à partir du code de votre fonction Lambda.

Création d'une fonction qui écrit des journaux

Pour produire des journaux à partir du code de votre fonction, vous pouvez utiliser n'importe quelle fonction de journalisation qui écrit dans `stdout` ou `stderr`, comme la macro `println!`. L'exemple suivant utilise `println!` pour imprimer un message lorsque le gestionnaire de fonction démarre et avant qu'il ne se termine.

```
use lambda_runtime::{service_fn, LambdaEvent, Error};
use serde_json::{json, Value};
async fn handler(event: LambdaEvent<Value>) -> Result<Value, Error> {
    println!("Rust function invoked");
    let payload = event.payload;
    let first_name = payload["firstName"].as_str().unwrap_or("world");
    println!("Rust function responds to {}", &first_name);
    Ok(json!({ "message": format!("Hello, {first_name}!") }))
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    lambda_runtime::run(service_fn(handler)).await
}
```

Implémentation de la journalisation avancée avec la caisse Tracing

Tracing est un cadre permettant d'instrumenter les programmes Rust afin de collecter des informations de diagnostic structurées et basées sur des événements. Ce cadre fournit des utilitaires pour personnaliser les niveaux et les formats de sortie des journaux, comme la création de messages de journal JSON structurés. Pour utiliser ce cadre, vous devez initialiser un `subscriber` avant de

mettre en œuvre le gestionnaire de fonction. Ensuite, vous pouvez utiliser des macros de traçage comme `debug`, `info` et `error` pour spécifier le niveau de journal que vous voulez pour chaque scénario.

Example– Utilisation de la caisse Tracing

Notez ce qui suit :

- `tracing_subscriber::fmt().json()` : lorsque cette option est incluse, les journaux sont formatés en JSON. Pour utiliser cette option, vous devez inclure la fonction `json` dans la dépendance `tracing-subscriber` (par exemple, `tracing-subscriber = { version = "0.3.11", features = ["json"] }`).
- `#[tracing::instrument(skip(event), fields(req_id = %event.context.request_id))]` : cette annotation génère une étendue à chaque fois que le gestionnaire est invoqué. L'étendue ajoute l'identifiant de la demande à chaque ligne de journal.
- `{ %first_name }` : cette construction ajoute le champ `first_name` à la ligne de journal où il est utilisé. La valeur de ce champ correspond à la variable du même nom.

```
use lambda_runtime::{service_fn, Error, LambdaEvent};
use serde_json::{json, Value};
#[tracing::instrument(skip(event), fields(req_id = %event.context.request_id))]
async fn handler(event: LambdaEvent<Value>) -> Result<Value, Error> {
    tracing::info!("Rust function invoked");
    let payload = event.payload;
    let first_name = payload["firstName"].as_str().unwrap_or("world");
    tracing::info!({ %first_name }, "Rust function responds to event");
    Ok(json!({ "message": format!("Hello, {first_name}!") }))
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    tracing_subscriber::fmt().json()
        .with_max_level(tracing::Level::INFO)
        // this needs to be set to remove duplicated information in the log.
        .with_current_span(false)
        // this needs to be set to false, otherwise ANSI color codes will
        // show up in a confusing manner in CloudWatch logs.
        .with_ansi(false)
        // disabling time is handy because CloudWatch will add the ingestion time.
        .without_time()
```

```
        // remove the name of the function from every log entry
        .with_target(false)
        .init();
    lambda_runtime::run(service_fn(handler)).await
}
```

Lorsque cette fonction Rust est invoquée, elle imprime deux lignes de journal similaires à ce qui suit :

```
{"level":"INFO","fields":{"message":"Rust function invoked"},"spans":
[{"req_id":"45daaaa7-1a72-470c-9a62-e79860044bb5","name":"handler"}]}
{"level":"INFO","fields":{"message":"Rust function responds to
 event","first_name":"David"},"spans":[{"req_id":"45daaaa7-1a72-470c-9a62-
e79860044bb5","name":"handler"}]}
```

Exécutions de la fonction Lambda Event

AWS Lambda Les fonctions événementielles (précédemment appelées fonctions Lambda) prennent en charge plusieurs langues grâce à temps d'exécution. Une exécution fournit un environnement spécifique au langage qui relaie les événements d'invocation, les informations de contexte et les réponses entre Lambda et la fonction. Vous pouvez utiliser les runtimes que Lambda fournit, ou créer vos propres runtimes. Pour plus d'informations sur les environnements d'exécution open source, voir the section called “Référentiels open source”. Pour les environnements d'exécution utilisés par Lambda Web Functions, voir the section called “Runtimes ”.

Lambda est indépendant de votre choix d’environnement d’exécution. Pour les fonctions simples, les langages interprétés tels que Python et Node.js offrent les performances les plus rapides. Pour les fonctions nécessitant des calculs plus complexes, les langages compilés tels que Java sont souvent plus lents à initialiser, mais s’exécutent rapidement dans le gestionnaire Lambda. Le choix de l’environnement d’exécution dépend également des préférences du développeur et de sa connaissance du langage.

Chaque version majeure du langage de programmation possède un environnement d’exécution distinct, avec un identifiant de l’environnement d’exécution unique, tel que `nodejs24.x` ou `python3.14`. Pour configurer une fonction afin d’utiliser une nouvelle version majeure du langage, vous devez modifier l’identifiant d’exécution. Depuis AWS Lambda ne peut garantir la rétrocompatibilité entre les versions majeures, il s'agit d'une opération pilotée par le client.

Pour une fonction définie en tant qu'image de conteneur, vous choisissez une exécution et la distribution Linux lorsque vous créez l'image de conteneur. Pour modifier l'environnement d'exécution, vous créez une image de conteneur.

Lorsque vous utilisez une archive de fichiers .zip pour le package de déploiement, vous choisissez un environnement d'exécution lorsque vous créez la fonction. Pour modifier l'environnement d'exécution, vous pouvez mettre à jour la configuration de votre fonction. L'environnement d'exécution est associé à l'une des distributions Amazon Linux. L'environnement d'exécution sous-jacent fournit des bibliothèques et des variables d'environnement supplémentaires auxquelles vous pouvez accéder depuis le code de votre fonction.

Lambda invoque votre fonction dans un environnement d'exécution. L'environnement d'exécution fournit un environnement d'environnement d'exécution sécurisé et isolé qui gère les ressources nécessaires à l'exécution de votre fonction. Lambda réutilise l'environnement d'exécution à partir d'une invocation antérieure dans le cas où il y en a un disponible, ou il peut en créer un nouveau.

Pour utiliser d'autres langages dans Lambda, tels que Va ou Rouille, utilisez un OS-only exécution. L'environnement d'exécution de Lambda fournit une interface d'environnement d'exécution pour obtenir des événements d'invocations et envoyer des réponses. Vous pouvez déployer les autres langages en implémentant un environnement d'exécution en association avec le code de votre fonction, ou dans une couche.

Environnements d'exécution pris en charge

Le tableau suivant répertorie les environnements d'exécution Lambda pris en charge pour Event Functions et les dates de dépréciation prévues. Une fois qu'un environnement d'exécution est obsolète, vous pouvez toujours créer et mettre à jour des fonctions pendant une période limitée. Pour plus d'informations, consultez the section called "Environnement d'exécution utilisé après la date d'obsolescence". Le tableau fournit les dates actuellement prévues pour la dépréciation de l'exécution sur la base de notre the section called "politique d'obsolescence de l'exécution". Ces dates sont fournies à des fins de planification et sont susceptibles d'être modifiées.

> **Note**
>
> Le Node.js Les environnements d'exécution 2.6 et Python 3.15 sont disponibles aperçu public. Les temps d'exécution de la version préliminaire ne sont pas couverts par le SLA Lambda ni par le support technique et ne doivent pas être utilisés pour les charges de travail de production.

L'objectif des versions préliminaires est de recueillir les commentaires des clients, des partenaires et des communautés linguistiques en amont avant la mise en disponibilité générale, tout en restant possible. Vous pouvez faire part de vos commentaires via le GitHub problèmes pour Node.js 26 et Python 3.15. Pour plus d'informations, consultez ce billet de blog.

Important

La fin de vie d'Amazon Linux 2 est prévue pour le 30 juin 2026. Les environnements d'exécution Lambda et les images de base de conteneurs pour Java 8 (AL2), Java 11 (AL2), Java 17 (AL2), Python 3.10, Python 3.11 et provid.al2 continueront à recevoir des correctifs pour critique et sélectionné important Problèmes de sécurité liés à Amazon Linux 2, en plus des correctifs d'exécution du langage, jusqu'aux dates de dépréciation indiquées dans le tableau ci-dessous.

Nous recommandons aux clients de passer à un environnement d'exécution basé sur Amazon Linux 2023 dès que possible. Pour les clients effectuant une mise à niveau vers Java 21 ou Java 25, vous pouvez utiliser AWS Transform personnalisé pour vous aider à effectuer ces mises à niveau. Pour les clients qui ne peuvent pas mettre à niveau leur version Java, nous proposons des environnements d'exécution basés sur Amazon Linux 2023 pour Java 8, Java 11 et Java 17 qui suivent le calendrier de dépréciation AL2023.

Nom	Identifiant	Système d'exploitation	Date d'obsolescence	Créer la fonction de blocage	Mettre à jour la fonction de blocage
Node.js 26	`nodejs26.x`	Amazon Linux 2	Non planifié	Non planifié	Non planifié
Node.js 24	`nodejs24.x`	Amazon Linux 2	30 avril 2028	1 juin 2028	1 juillet 2028
Node.js 22	`nodejs22.x`	Amazon Linux 2	30 avril 2027	29 juillet 2027	31 août 2027

Nom	Identifiant	Système d'exploitation	Date d'obsolescence	Créer la fonction de blocage	Mettre à jour la fonction de blocage
Python 3.15	`python3.15`	Amazon Linux 2	Non planifié	Non planifié	Non planifié
Python 3.14	`python3.14`	Amazon Linux 2	30 juin 2029	31 juillet 2029	31 août 2029
Python 3.13	`python3.13`	Amazon Linux 2	30 juin 2029	31 juillet 2029	31 août 2029
Python 3.12	`python3.12`	Amazon Linux 2	31 octobre 2028	30 novembre 2028	10 janvier 2029
Python 3.11	`python3.11`	Amazon Linux 2	30 juin 2027	29 juillet 2027	31 août 2027
Python 3.10	`python3.10`	Amazon Linux 2	31 octobre 2026	29 juillet 2027	31 août 2027
Java 25	`java25`	Amazon Linux 2	30 juin 2029	31 juillet 2029	31 août 2029
Java 21	`java21`	Amazon Linux 2	30 juin 2029	31 juillet 2029	31 août 2029
Java 17	`java17.al2023`	Amazon Linux 2	30 juin 2029	31 juillet 2029	31 août 2029
Java 11	`java11.al2023`	Amazon Linux 2	30 juin 2029	31 juillet 2029	31 août 2029
Java 8	`java8.al2023`	Amazon Linux 2	30 juin 2029	31 juillet 2029	31 août 2029
Java 17	`java17`	Amazon Linux 2	30 juin 2027	29 juillet 2027	31 août 2027
Java 11	`java11`	Amazon Linux 2	30 juin 2027	29 juillet 2027	31 août 2027

Nom	Identifiant	Système d'exploitation	Date d'obsolescence	Créer la fonction de blocage	Mettre à jour la fonction de blocage
Java 8	`java8.al2`	Amazon Linux 2	30 juin 2027	29 juillet 2027	31 août 2027
.NET 10	`dotnet10`	Amazon Linux 2	14 novembre 2028	14 décembre 2028	15 janvier 2029
.NET 9 (conteneur uniquement)	`dotnet9`	Amazon Linux 2	10 novembre 2026	Non planifié	Non planifié
.NET 8	`dotnet8`	Amazon Linux 2	10 novembre 2026	29 juillet 2027	31 août 2027
Ruby 4.0	`ruby4.0`	Amazon Linux 2	31 mars 2029	30 avril 2029	31 mai 2029
Ruby 3.4	`ruby3.4`	Amazon Linux 2	31 mars 2028	30 avril 2028	31 mai 2028
Ruby 3.3	`ruby3.3`	Amazon Linux 2	31 mars 2027	29 juillet 2027	31 août 2027
OS-only Durée d'exécution	`provided.al2023`	Amazon Linux 2	30 juin 2029	31 juillet 2029	31 août 2029

> **Note**
>
> Pour les nouvelles régions, Lambda ne prendra pas en charge les environnements d'exécution qui devraient devenir obsolètes dans les six prochains mois.

Lambda tient à jour les environnements d'exécution gérés et de leurs images de conteneur correspondantes à jour grâce à des correctifs et à la prise en charge des versions mineures. Pour plus d'informations, consultez Mises à jour de l'exécution Lambda.

Pour interagir par programmation avec d'autres Services AWS et les ressources de votre fonction, vous pouvez utiliser l'un des AWS SDK. Le Node.js, Python et Ruby incluent une version du AWS SDK. Toutefois, pour conserver le contrôle total de vos dépendances et optimiser la rétrocompatibilité lors des mises à jour automatiques de l'exécution, nous vous recommandons de toujours inclure les modules SDK utilisés par votre code (ainsi que les dépendances éventuelles) dans le package de déploiement de votre fonction ou dans une couche Lambda.

Nous vous recommandons d'utiliser la version du SDK incluant l'environnement d'exécution uniquement lorsque vous ne pouvez pas inclure de packages supplémentaires dans votre déploiement, Par exemple, lorsque vous créez votre fonction à l'aide de l'éditeur de code de la console Lambda ou que vous utilisez le code de fonction en ligne dans CloudFormation modèle.

Lambda met régulièrement à jour les versions du AWS SDK inclus dans Node.js, Python et Ruby runtimes. Pour déterminer la version du SDK AWS incluse dans l'environnement d'exécution que vous utilisez, consultez les sections suivantes :

- Runtime-included Versions du SDK (Node.js)
- Runtime-included Versions du SDK (Python)
- Runtime-included Versions du SDK (Ruby)

Lambda continue de prendre en charge le langage de programmation Go après l'obsolescence de l'environnement d'exécution Go 1.x. Pour plus d'informations, voir Migration AWS Lambda fonctions du Go1.x exécution vers l'environnement d'exécution personnalisé sur Amazon Linux 2 sur le AWS Blog informatique.

Tous les environnements d'exécution Lambda pris en charge supportent les architectures x86_64 et arm64.

Nouvelles versions d'exécution

Lambda fournit des environnements d'exécution gérés pour les nouvelles versions de langage uniquement lorsque la version atteint la phase LTS (support à long terme) du cycle de distribution du langage. Par exemple, pour Node.js cycle de publication, lorsque la version atteint la phase Active LTS.

Avant que la version n'atteigne la phase de support à long terme, elle reste en développement et peut encore faire l'objet de modifications majeures. Lambda applique automatiquement les mises à jour d'environnements d'exécution par défaut, de sorte que l'interruption des modifications apportées à une version d'environnement d'exécution peut empêcher vos fonctions de fonctionner comme prévu.

Lambda ne fournit pas d'environnements d'exécution gérés pour les versions linguistiques dont la sortie du LTS n'est pas prévue.

La liste suivante montre le mois de lancement cible pour les environnements d'exécution Lambda à venir. Ces dates ne sont données qu'à titre indicatif et sont susceptibles d'être modifiées.

- Node.js 26 - novembre 2026
- Python 3.15 - novembre 2026

politique d'obsolescence de l'exécution

Les environnements d'exécution Lambda pour les archives de fichiers .zip combinent un système d'exploitation, un langage de programmation et des bibliothèques de logiciels qui font l'objet d'une maintenance et de mises à jour de sécurité. La politique de dépréciation standard de Lambda consiste à rendre obsolète un environnement d'exécution lorsqu'un composant majeur de celui-ci atteint la fin du support communautaire à long terme (LTS) et que les mises à jour de sécurité ne sont plus disponibles. Le plus souvent, il s'agit de l'environnement d'exécution du langage, bien que dans certains cas, un environnement d'exécution puisse être obsolète car le système d'exploitation (OS) atteint la fin du LTS.

Une fois qu'un runtime est devenu obsolète, AWS peut ne plus appliquer de correctifs de sécurité ou de mises à jour à ce runtime, et les fonctions utilisant ce runtime ne sont plus éligibles au support technique. Ces environnements d'exécution obsolètes sont fournis « tels quels », sans aucune garantie, et peuvent contenir des bogues, des erreurs, des défauts ou d'autres vulnérabilités.

Pour en savoir plus sur la gestion des mises à niveau et de la dépréciation de l'environnement d'exécution, consultez les sections suivantes et Gérer AWS Lambda mises à niveau du runtime sur le AWS Blog informatique.

> **Important**
>
> Lambda retarde parfois l'obsolescence d'un environnement d'exécution Lambda pendant une période limitée au-delà de la date de fin du support de la version du langage prise en charge par l'environnement d'exécution. Pendant cette période, Lambda applique uniquement des correctifs de sécurité au système d'exploitation de l'environnement d'exécution. Lambda n'applique pas de correctifs de sécurité aux environnements d'exécution des langages de programmation une fois leur date de fin de support atteinte.

Modèle de responsabilité partagée

Lambda est responsable de la conservation et de la publication des mises à jour de sécurité pour tous les environnements d'exécution gérés et les images de base de conteneur pris en charge. Par défaut, Lambda appliquera ces mises à jour automatiquement aux fonctions utilisant des environnements d'exécution gérés. Lorsque le paramètre de mise à jour automatique de l'environnement d'exécution par défaut a été modifié, consultez le modèle de responsabilité partagée des contrôles de gestion de l'environnement d'exécution. Pour les fonctions déployées à l'aide d'images de conteneurs, vous êtes responsable de la reconstruction de l'image de conteneur de votre fonction à partir de la dernière image de base et du redéploiement de l'image de conteneur.

Lorsqu'un environnement d'exécution est obsolète, la responsabilité de Lambda en matière de mise à jour du runtime géré et des images de base de conteneurs cesse. Vous êtes responsable de la mise à niveau de vos fonctions afin d'utiliser un environnement d'exécution ou une image de base compatible.

Dans tous les cas, vous êtes responsable de l'application des mises à jour de votre code de fonction, y compris ses dépendances. Vos responsabilités dans le cadre du modèle de responsabilité partagée sont résumées dans le tableau suivant.

Phase de cycle de vie de l'environnement d'exécution	Responsabilité de Lambda	Vos responsabilités
Environnement d'exécution géré pris en charge	Fournissez des mises à jour d'environnement d'exécution régulières avec des correctifs de sécurité et d'autres mises à jour. Appliquer les mises à jour de l'environnement d'exécution automatiquement par défaut (consultez the section called "Modes de mise à jour de l'environnement d'exécution" pour les comportements autres que ceux par défaut).	Mettez à jour votre code de fonction, y compris ses dépendances, pour corriger les éventuelles failles de sécurité.

Phase de cycle de vie de l'environnement d'exécution	Responsabilité de Lambda	Vos responsabilités
Image de conteneur prise en charge	Fournissez des mises à jour régulières de l'image de base du conteneur avec des correctifs de sécurité et autres mises à jour.	Mettez à jour votre code de fonction, y compris ses dépendances, pour corriger les éventuelles failles de sécurité. Reconstruisez et redéploye z régulièrement votre image de conteneur à l'aide de la dernière image de base.
Environnement d'exécution géré proche de l'obsolescence	Avertissez les clients avant la dépréciation de l'exécution par le biais de la documenta tion, Tableau de bord Health, e-mail et Trusted Advisor. La responsabilité des mises à jour de l'environnement d'exécution prend fin en cas d'obsolescence.	Surveillez la documenta tion Lambda, Tableau de bord Health, e-mail ou Trusted Advisor pour obtenir des informations sur la dépréciat ion de l'exécution. Mettez à niveau les fonctions vers un environnement d'exécution compatible avant que le précédent ne soit obsolète.
L'image de conteneur approche de l'obsolescence	Les notifications d'obsoles cence ne sont pas disponibles pour les fonctions utilisant des images de conteneur. La responsabilité des mises à jour de l'image de base du conteneur s'arrête à la date d'obsolescence.	Tenez compte des planifica tions d'obsolescence et mettez à niveau les fonctions vers une image de base prise en charge avant que l'image précédente ne soit obsolète.

Environnement d’exécution utilisé après la date d’obsolescence

Une fois qu'un runtime est devenu obsolète, AWS peut ne plus appliquer de correctifs de sécurité ou de mises à jour à ce runtime, et les fonctions utilisant ce runtime ne sont plus éligibles au support technique. Bien que vous puissiez continuer à invoquer vos fonctions indéfiniment, AWS recommande vivement de migrer vers un environnement d'exécution pris en charge. Les environnements d’exécution obsolètes sont fournis « en l’état », sans aucune garantie, et peuvent contenir des bogues, des erreurs, des défauts ou d’autres vulnérabilités. Les fonctions qui utilisent un environnement d’exécution obsolète peuvent subir une dégradation des performances ou d’autres problèmes, tels que l’expiration d’un certificat, qui peuvent les empêcher de fonctionner correctement.

Vous pouvez mettre à jour une fonction pour qu’elle utilise un environnement d’exécution plus récent à tout moment après qu’un environnement d’exécution soit devenu obsolète. Nous vous recommandons de tester votre fonction avec le nouveau moteur d’exécution avant d’appliquer les modifications aux environnements de production. Vous ne pourrez plus revenir à l’environnement d’exécution obsolète une fois les mises à jour des fonctions bloquées. Nous vous recommandons d’utiliser des versions et alias de fonctions pour permettre un déploiement sécurisé avec restauration.

La chronologie suivante décrit ce qui se produit lorsqu’un environnement d’exécution est obsolète :

Phase de cycle de vie de l’environnement d’exécution	Lorsque	Quoi
Période d’avis d’obsolescence	Au moins 180 jours avant l’obsolescence	• AWS envoie des notifications par e-mail et Tableau de bord Health aux comptes dont les fonctions utilisent ce moteur d'exécution dans leur `$LATEST` version. • Les fonctions concernées sont également répertoriées dans l’onglet Modifications planifiées de Tableau de bord Health et dans la vérification des environnements d’exécution obsolètes AWS Trusted Advisor.
Obsolescence	Date d’obsolescence	• AWS peut ne plus appliquer les mises à jour de sécurité ou autres mises à jour. • Les fonctions ne sont plus éligibles au support technique.

Phase de cycle de vie de l'environnement d'exécution	Lorsque	Quoi
		• Vous ne pouvez plus créer ou mettre à jour de fonctions à l'aide de l'environnement d'exécution obsolète de la console Lambda. Vous pouvez continuer à créer et à mettre à jour des fonctions via AWS CLI, AWS SAM, ou CloudFormation.
Créer la fonction de blocage	Au moins 30 jours après l'obsolescence	• Lambda commence à bloquer la création de nouvelles fonctions. • Vous pouvez continuer à mettre à jour le code et la configuration des fonctions existantes via AWS CLI, AWS SAM, ou CloudFormation..
Mettre à jour la fonction de blocage	Au moins 60 jours après l'obsolescence	• Lambda commence à bloquer la mise à jour du code et de la configuration pour les fonctions existantes. • Vous pouvez toujours mettre à niveau la configuration des fonctions vers un environnement d'exécution compatible. Cependant, le retour à l'environnement d'exécution obsolète pourrait être bloqué.

> **Note**
>
> Pour certains temps d'exécution, AWS retarde les dates de création et de mise à jour des fonctions de bloc au-delà des 30 et 60 jours habituels après la dépréciation. AWS a effectué cette modification en réponse aux commentaires des clients afin de vous donner plus de temps pour mettre à jour vos fonctions. Reportez-vous aux tableaux figurant dans the section called "Environnements d'exécution pris en charge" et the section called "Environnements d'exécution obsolètes" pour connaître les dates relatives à votre environnement d'exécution.

Lambda ne commencera pas à bloquer les créations ou les mises à jour de fonctions avant les dates indiquées dans ces tables.

Réception de notifications d'obsolescence lors de l'exécution

Lorsqu'un environnement d'exécution approche de sa date de dépréciation, Lambda vous envoie une alerte par e-mail si l'une des fonctions de votre Compte AWS utilisez ce runtime. Les notifications sont également affichées dans le Tableau de bord Health et dans AWS Trusted Advisor.

- Réception de notifications par e-mail :

  Lambda vous envoie une alerte par e-mail au moins 180 jours avant qu'un environnement d'exécution ne soit obsolète. Cet e-mail répertorie les versions $LATEST de toutes les fonctions utilisant le runtime. Pour consulter la liste complète des versions des fonctions concernées, utilisez Trusted Advisor ou voir the section called “Obtenir des données sur les fonctions par environnement d’exécution”.

  Lambda envoie une notification par e-mail à votre Compte AWS contact principal du compte. Pour plus d'informations sur l'affichage ou la mise à jour des adresses e-mail de votre compte, consultez la section Mise à jour des informations de contact dans la Référence générale AWS .
- Recevoir des notifications via le Tableau de bord Health:

  Le Tableau de bord Health affiche au moins une notification 180 jours avant qu'un environnement d'exécution ne soit obsolète. Les notifications apparaissent sur la page État de votre compte sous Autres notifications. L'onglet Ressources affectées de la notification répertorie les versions $LATEST de toutes les fonctions utilisant le runtime.

  > **Note**
  >
  > Pour consulter la liste complète et à jour des versions des fonctions concernées, utilisez Trusted Advisor ou voir the section called “Obtenir des données sur les fonctions par environnement d’exécution”.

  Tableau de bord Health les notifications expirent 90 jours après la dépréciation de l'environnement d'exécution concerné.
- En utilisant AWS Trusted Advisor

Trusted Advisor affiche au moins une notification 180 jours avant qu'un environnement d'exécution ne soit obsolète. Les notifications apparaissent sur la page Sécurité. La liste des fonctions concernées s'affiche sous Fonctions AWS Lambda utilisant des environnements d'exécution obsolètes. Cette liste de fonctions affiche à la fois $LATEST et les versions publiées et les mises à jour automatiques pour refléter l'état actuel de vos fonctions.

Vous pouvez activer les notifications hebdomadaires par e-mail depuis Trusted Advisor dans le Préférences page du Trusted Advisor console.

Environnements d’exécution obsolètes

Les environnements d’exécution suivants ont atteint la fin de prise en charge :

Nom	Identifiant	Système d’exploitation	Date d’obsolescence	Créer la fonction de blocage	Mettre à jour la fonction de blocage
OS-only Durée d'exécution	`provided.al2`	Amazon Linux 2	31 juillet 2026	29 juillet 2027	31 août 2027
Node.js 20	`nodejs20.x`	Amazon Linux 2	30 avril 2026	29 juillet 2027	31 août 2027
Ruby 3.2	`ruby3.2`	Amazon Linux 2	31 mars 2026	29 juillet 2027	31 août 2027
Python 3.9	`python3.9`	Amazon Linux 2	15 décembre 2025	29 juillet 2027	31 août 2027
Node.js 18	`nodejs18.x`	Amazon Linux 2	1e septembre 2	29 juillet 2027	31 août 2027
.NET 6	`dotnet6`	Amazon Linux 2	20 décembre 2(	29 juillet 2027	31 août 2027
Python 3.8	`python3.8`	Amazon Linux 2	14 octobre 202	29 juillet 2027	31 août 2027

Nom	Identifiant	Système d'exploitation	Date d'obsolescence	Créer la fonction de blocage	Mettre à jour la fonction de blocage
Node.js 16	`nodejs16.x`	Amazon Linux 2	12 juin 2024	29 juillet 2027	31 août 2027
.NET 7 (conteneur uniquement)	`dotnet7`	Amazon Linux 2	14 mai 2024	N/A	N/A
Java 8	`java8`	Amazon Linux	8 janvier 2024	8 février 2024	31 août 2027
Go 1.x	`go1.x`	Amazon Linux	8 janvier 2024	8 février 2024	31 août 2027
OS-only Durée d'exécution	`provided`	Amazon Linux	8 janvier 2024	8 février 2024	31 août 2027
Ruby 2.7	`ruby2.7`	Amazon Linux 2	7 décembre 20	9 janvier 2024	31 août 2027
Node.js 14	`nodejs14.x`	Amazon Linux 2	4 décembre 20	9 janvier 2024	31 août 2027
Python 3.7	`python3.7`	Amazon Linux	4 décembre 20	9 janvier 2024	31 août 2027
.NET Core 3.1	`dotnetcore3.1`	Amazon Linux 2	3 avril 2023	3 avril 2023	3 mai 2023
Node.js 12	`nodejs12.x`	Amazon Linux 2	31 mars 2023	31 mars 2023	30 avril 2023
Python 3.6	`python3.6`	Amazon Linux	18 juillet 2022	18 juillet 2022	29 août 2022

Nom	Identifiant	Système d'exploitation	Date d'obsolescence	Créer la fonction de blocage	Mettre à jour la fonction de blocage
.NET 5 (conteneur uniquement)	`dotnet5.0`	Amazon Linux 2	10 mai 2022	N/A	N/A
.NET Core 2.1	`dotnetcore2.1`	Amazon Linux	5 janvier 2022	5 janvier 2022	13 avril 2022
Node.js 10	`nodejs10.x`	Amazon Linux 2	30 juillet 2021	30 juillet 2021	14 février 2022
Ruby 2.5	`ruby2.5`	Amazon Linux	30 juillet 2021	30 juillet 2021	31 mars 2022
Python 2.7	`python2.7`	Amazon Linux	15 juillet 2021	15 juillet 2021	30 mai 2022
Node.js 8,10	`nodejs8.10`	Amazon Linux	6 mars 2020	4 février 2020	6 mars 2020
Node.js 4.3	`nodejs4.3`	Amazon Linux	5 mars 2020	3 février 2020	5 mars 2020
Node.js 4.3 bord	`nodejs4.3-edge`	Amazon Linux	5 mars 2020	31 mars 2019	30 avril 2019
Node.js 6,10	`nodejs6.10`	Amazon Linux	12 août 2019	12 juillet 2019	12 août 2019
.NET Core 1.0	`dotnetcore1.0`	Amazon Linux	27 juin 2019	30 juin 2019	30 juillet 2019
.NET Core 2.0	`dotnetcore2.0`	Amazon Linux	30 mai 2019	30 avril 2019	30 mai 2019

Nom	Identifiant	Système d'exploitation	Date d'obsolescence	Créer la fonction de blocage	Mettre à jour la fonction de blocage
Node.js 0,10	`nodejs`	Amazon Linux	30 août 2016	30 septembre 2016	31 octobre 2016

Dans la plupart des cas, la date de fin de vie d'une version de langage ou d'un système d'exploitation est bien connue à l'avance. Les liens ci-dessous donnent les calendriers de fin de vie pour chaque langage que Lambda prend en charge en tant qu'environnement d'exécution géré.

Stratégies de prise en charge des langages et des infrastructures

- Node.js — github.com
- Python – devguide.python.org
- Ruby – www.ruby-lang.org
- Java – www.oracle.com et Corretto FAQs
- Go – golang.org
- .NET – dotnet.microsoft.com

Comprendre comment Lambda gère les mises à jour de version de l'environnement d'exécution

Lambda maintient à jour chaque environnement d'exécution géré avec des mises à jour de sécurité, des corrections de bogues, de nouvelles fonctionnalités, des améliorations de performance et la prise en charge des versions mineures. Ces mises à jour d'environnement d'exécution sont publiées sous forme de versions d'environnement d'exécution. Lambda applique les mises à jour d'exécution à Event Functions en migrant la fonction d'une version d'exécution antérieure vers une nouvelle version d'exécution.

Par défaut, pour les fonctions utilisant des exécutions gérées, Lambda applique des mises à jour automatiquement. Avec les mises à jour de l'environnement d'exécution automatiques, Lambda prend en charge la charge opérationnelle de l'application de correctifs aux versions de l'environnement d'exécution. Pour la plupart des clients, les mises à jour automatiques sont le bon choix. Vous pouvez modifier ce comportement par défaut en configurant les paramètres de gestion de l'environnement d'exécution.

Lambda publie également chaque nouvelle version de l'environnement d'exécution sous forme d'image de conteneur. Pour mettre à jour les versions des environnements d'exécution pour les fonctions basées sur des conteneurs, vous devez créer une nouvelle image de conteneur à partir de l'image de base mise à jour et redéployer votre fonction.

Chaque version de l'environnement d'exécution est associée à un numéro de version et à un ARN (Amazon Resource Name). Les numéros de version de l'environnement d'exécution utilisent un schéma de numérotation que Lambda définit, indépendamment des numéros de version utilisés par le langage de programmation. Les numéros de version des environnements d'exécution ne sont pas toujours séquentiels. Par exemple, la version 42 peut être suivie de la version 45. L'ARN de la version de l'environnement d'exécution est un identifiant unique pour chaque version. Vous pouvez voir l'ARN de la version de l'environnement d'exécution actuelle de votre fonction dans la console Lambda ou dans la ligne `INIT_START` des journaux de votre fonction. Pour plus d'informations sur la gestion des mises à jour d'exécution dans les applications critiques, consultezthe section called "Permissions".

Les versions des environnements d'exécution ne doivent pas être confondues avec les identifiants des environnements d'exécution. Chaque environnement d'exécution possède un identifiant unique, tel que `python3.14` ou `nodejs24.x`. Ceux-ci correspondent à chaque version majeure du langage de programmation. Les versions de l'environnement d'exécution décrivent la version corrective d'un environnement d'exécution individuel.

> **Note**
>
> L'ARN pour le même numéro de version d'exécution peut varier selon Régions AWS les architectures de processeur.

Rubriques

- Rétrocompatibilité
- Modes de mise à jour de l’environnement d’exécution
- Two-phase déploiement de la version d'exécution
- Configuration des paramètres de gestion de l’environnement d’exécution Lambda
- Rétablissement d’une version de l’environnement d’exécution Lambda
- Identification des changements de version de l’environnement d’exécution Lambda
- Comprendre le modèle de responsabilité partagée pour la gestion des environnements d’exécution Lambda
- Contrôle des autorisations de mise à jour de l’environnement d’exécution Lambda pour les applications hautement conformes

Rétrocompatibilité

Lambda s’efforce de fournir des mises à jour d’environnement d’exécution qui sont rétrocompatibles avec les fonctions existantes. Cependant, comme pour les correctifs logiciels, il existe de rares cas dans lesquels une mise à jour de l’environnement d’exécution peut avoir un impact négatif sur une fonction existante. Par exemple, les correctifs de sécurité peuvent exposer un problème sous-jacent à une fonction existante qui dépend du comportement précédent, non sécurisé.

Lorsque vous créez et déployez votre fonction, il est important de comprendre comment gérer vos dépendances afin d’éviter d’éventuelles incompatibilités lors d’une future mise à jour d’environnement d’exécution. Supposons, par exemple, que votre fonction soit dépendante du package A, lui-même dépendant du package B. Les deux packages sont inclus dans l’environnement d’exécution Lambda (par exemple, ils peuvent faire partie du SDK ou de ses dépendances, ou faire partie des bibliothèques du système d’exécution).

Réfléchissez aux scénarios suivants :

Déploiement	Compatible avec les correctifs	Raison
• Package A : utilisation depuis l'environnement d'exécution • Package B : utilisation depuis l'environnement d'exécution	Oui	Les futures mises à jour d'environnement d'exécution des packages A et B seront rétrocompatibles.
• Package A : dans le package de déploiement • Package B : dans le package de déploiement	Oui	Votre déploiement étant prioritaire, les futures mises à jour d'environnement d'exécuti on des packages A et B n'auront aucun effet.
• Package A : dans le package de déploiement • Package B : utilisation depuis l'environnement d'exécution	Oui*	Les futures mises à jour d'environnement d'exécuti on du package B seront rétrocompatibles. *Si A et B sont étroitement couplés, des problèmes de compatibilité peuvent survenir. Par exemple, les `botocore` packages `boto3` et du AWS SDK pour Python doivent être déployés ensemble.
• Package A : utilisation depuis l'environnement d'exécution • Package B : dans le package de déploiement	Non	Les futures mises à jour d'environnement d'exécuti on du package A peuvent nécessiter une version mise à jour du package B. Cependant , la version déployée du package B est prioritaire et risque de ne pas être

Déploiement	Compatible avec les correctifs	Raison
		compatible avec la version mise à jour du package A.

Pour maintenir la compatibilité avec les futures mises à jour d'environnement d'exécution, suivez les bonnes pratiques suivantes :

- Dans la mesure du possible, regroupez toutes les dépendances : incluez toutes les bibliothèques requises, y compris le AWS SDK et ses dépendances, dans votre package de déploiement. Cela garantit que votre ensemble de composants reste stable et compatible.
- Utilisez les SDK fournis par l'exécution avec parcimonie : ne vous fiez au SDK fourni par l'exécution que lorsque vous ne pouvez pas inclure de packages supplémentaires (par exemple, lorsque vous utilisez l'éditeur de code de la console Lambda ou du code en ligne dans un modèle). AWS CloudFormation
- Évitez de remplacer les bibliothèques système : ne déployez pas de bibliothèques de système d'exploitation personnalisées susceptibles d'entrer en conflit avec les futures mises à jour d'exécution.

Modes de mise à jour de l'environnement d'exécution

Lambda s'efforce de fournir des mises à jour d'environnement d'exécution qui sont rétrocompatibles avec les fonctions existantes. Cependant, comme pour les correctifs logiciels, il existe de rares cas dans lesquels une mise à jour de l'environnement d'exécution peut avoir un impact négatif sur une fonction existante. Par exemple, les correctifs de sécurité peuvent exposer un problème sous-jacent à une fonction existante qui dépend du comportement précédent, non sécurisé. Les contrôles de gestion de l'environnement d'exécution Lambda permettent de réduire le risque d'impact sur vos charges de travail dans le cas rare d'une incompatibilité de version. Pour chaque version de fonction ($LATEST ou version publiée), vous pouvez choisir l'un des modes de mise à jour de l'environnement d'exécution suivants :

- Auto (par défaut) – Mettre automatiquement à jour vers la version de l'environnement d'exécution la plus sécurisée et la plus sûre à l'aide de Two-phase déploiement de la version d'exécution. Nous recommandons ce mode à la plupart des clients afin que vous puissiez toujours bénéficier des mises à jour de l'environnement d'exécution.

- Mise à jour de fonction – Mise à jour vers la version d'exécution la plus récente et la plus sécurisée lorsque vous mettez à jour votre fonction. Lorsque vous mettez à jour votre fonction, Lambda met à jour l'exécution de votre fonction vers la version la plus récente et la plus sécurisée. Cette approche synchronise les mises à jour de l'environnement d'exécution avec les déploiements de fonctions, ce qui vous permet de contrôler le moment où Lambda applique les mises à jour de l'environnement d'exécution. Avec ce mode, vous pouvez détecter et atténuer rapidement les rares incompatibilités de mise à jour de l'environnement d'exécution. Lorsque vous utilisez ce mode, vous devez régulièrement mettre à jour vos fonctions pour maintenir leur environnement d'exécution à jour.
- Manuel – Mise à jour manuelle de la version de votre exécution. Vous spécifiez une version de l'exécution dans la configuration de votre fonction. La fonction utilise cette version de l'environnement d'exécution indéfiniment.

  Dans les rares cas où une nouvelle version de l'environnement d'exécution est incompatible avec une fonction existante, vous pouvez utiliser ce mode pour ramener votre fonction à une version antérieure. Nous vous déconseillons d'utiliser le mode Manual (Manuel) pour tenter d'obtenir une cohérence de l'environnement d'exécution entre les déploiements. Pour plus d'informations, consultez Rétablissement d'une version de l'environnement d'exécution Lambda.

La responsabilité de l'application des mises à jour de l'environnement d'exécution à vos fonctions varie en fonction du mode de mise à jour que vous choisissez. Pour plus d'informations, consultez Comprendre le modèle de responsabilité partagée pour la gestion des environnements d'exécution Lambda.

Two-phase déploiement de la version d'exécution

Lambda introduit de nouvelles gestions des versions d'exécution dans l'ordre suivant :

1. Dans la première phase, Lambda applique la nouvelle version d'exécution chaque fois que vous créez ou mettez à jour une fonction. Une fonction est mise à jour lorsque vous appelez les opérations de UpdateFunctionConfigurationl'API UpdateFunctionCodeor.
2. Dans la deuxième phase, Lambda met à jour toute fonction qui utilise le mode de mise à jour Auto de l'environnement d'exécution et qui n'a pas encore été mise à jour vers la nouvelle version.

La durée totale du processus de déploiement varie en fonction de plusieurs facteurs, notamment la gravité de tout correctif de sécurité inclus dans la mise à jour de l'environnement d'exécution.

Si vous développez et déployez activement vos fonctions, il est fort probable que vous utilisiez de nouvelles versions d'exécution au cours de la première phase. Cela permet de synchroniser les mises à jour de l'environnement d'exécution avec les mises à jour des fonctions. Dans les rares cas où la dernière version d'exécution aurait un impact négatif sur votre application, cette approche vous permet de prendre rapidement des mesures correctives. Les fonctions qui ne sont pas en cours de développement bénéficient toujours des avantages opérationnels des mises à jour automatiques de l'environnement d'exécution au cours de la deuxième phase.

Cette approche n'affecte pas les fonctions définies en mode Function update (Mise à jour de fonction) ou en mode Manual (Manuel). Les fonctions utilisant le mode Function update (Mise à jour de fonction) reçoivent les dernières mises à jour de l'environnement d'exécution uniquement lorsque vous les créez ou les mettez à jour. Les fonctions utilisant le mode Manual (Manuel) ne reçoivent pas de mises à jour de l'environnement d'exécution.

Lambda publie les nouvelles versions de l'environnement d'exécution de manière progressive et continue à travers Régions AWS. Si vos fonctions sont réglées sur les modes de mise à jour automatique ou fonctionnelle, il est possible que les fonctions déployées simultanément dans différentes régions, ou à des moments différents dans la même région, utilisent différentes versions d'exécution. Les clients qui ont besoin de garantir la cohérence des versions d'exécution dans leurs environnements doivent utiliser des images de conteneur pour déployer leurs fonctions. Le mode Manuel est conçu comme une mesure d'atténuation temporaire pour permettre de restaurer la version d'exécution dans le rare cas où une version d'exécution est incompatible avec votre fonction.

Configuration des paramètres de gestion de l'environnement d'exécution Lambda

Vous pouvez configurer les paramètres de gestion de l'exécution pour vos fonctions d'événement Lambda à l'aide de la console Lambda ou du (). AWS Command Line Interface AWS CLI

> **Note**
>
> Vous pouvez configurer les paramètres de gestion de l'environnement d'exécution séparément pour chaque version de fonction.

Pour configurer la façon dont Lambda met à jour la version de votre environnement d'exécution (console)

1. Ouvrez la page Event Functions de la console Lambda.

2. Choisissez le nom d'une fonction événementielle.
3. Dans l'onglet Code, sous Runtime settings (Paramètres de l'environnement d'exécution), choisissez Edit runtime management configuration (Modifier la configuration de gestion de l'environnement d'exécution).
4. Sous Runtime management configuration (Configuration de la gestion de l'environnement d'exécution), choisissez l'une des options suivantes :

   - Pour que votre fonction se mette automatiquement à jour vers la dernière version de l'environnement d'exécution, sélectionnez Auto.
   - Pour que votre fonction se mette à jour vers la dernière version de l'environnement d'exécution lorsque vous modifiez la fonction, sélectionnez Function update (Mise à jour de fonction).
   - Pour que votre fonction soit mise à jour vers la dernière version de l'environnement d'exécution uniquement lorsque vous modifiez la version de l'environnement d'exécution ARN, sélectionnez Manual (Manuel). Vous trouverez l'ARN de la version de l'environnement d'exécution sous Runtime management configuration (Configuration de la gestion de l'environnement d'exécution). Vous pouvez également trouver l'ARN dans la ligne `INIT_START` des journaux de votre fonction.

   Pour de plus amples informations sur ces options, veuillez consulter Modes de mise à jour de l'environnement d'exécution.
5. Cliquez sur Enregistrer.

Pour configurer la façon dont Lambda met à jour votre version de l'environnement d'exécution (AWS CLI)

Pour configurer la gestion de l'exécution d'une fonction, exécutez la commande AWS CLI put-runtime-management-config. Lorsque vous utilisez le mode `Manual`, vous devez également fournir l'ARN de la version de l'environnement d'exécution.

```
aws lambda put-runtime-management-config \
  --function-name my-function \
  --update-runtime-on Manual \
  --runtime-version-arn arn:aws:lambda:us-
east-2::runtime:8eeff65f6809a3ce81507fe733fe09b835899b99481ba22fd75b5a7338290ec1
```

Vous devez voir des résultats similaires à ce qui suit :

```
{
  "UpdateRuntimeOn": "Manual",
  "FunctionArn": "arn:aws:lambda:us-east-2:111122223333:function:my-function",
  "RuntimeVersionArn": "arn:aws:lambda:us-
east-2::runtime:8eeff65f6809a3ce81507fe733fe09b835899b99481ba22fd75b5a7338290ec1"
}
```

Rétablissement d'une version de l'environnement d'exécution Lambda

Dans les rares cas où une nouvelle version d'exécution est incompatible avec votre fonction d'événement existante, vous pouvez restaurer sa version d'exécution à une version antérieure. Cela permet à votre application de continuer à fonctionner et de minimiser les perturbations, en laissant le temps de remédier à l'incompatibilité avant de revenir à la dernière version de l'environnement d'exécution.

Lambda n'impose pas de limite de temps à l'utilisation d'une version de l'environnement d'exécution particulière. Cependant, nous vous recommandons vivement de passer à la dernière version de l'environnement d'exécution dès que possible pour bénéficier des derniers correctifs de sécurité, des améliorations de performances et des fonctionnalités. Lambda offre la possibilité de revenir à une version antérieure de l'environnement d'exécution uniquement à titre d'atténuation temporaire dans le cas rare d'un problème de compatibilité de mise à jour de l'environnement d'exécution. Les fonctions qui utilisent une version d'exécution antérieure pendant une période prolongée peuvent éventuellement se heurter à une dégradation des performances ou à des problèmes, tels que l'expiration du certificat, qui peuvent les empêcher de fonctionner correctement.

Vous pouvez rétablir une version de l'environnement d'exécution de l'une des manières suivantes :

- En utilisant le mode de mise à jour Manual (Manuel) de l'environnement d'exécution
- En utilisant les versions de la fonction publiée

Pour plus d'informations, consultez la section Présentation des contrôles de gestion AWS Lambda d'exécution sur le blog AWS Compute.

Rétablissement d'une version de l'environnement d'exécution à l'aide du mode de mise à jour Manual (Manuel)

Si vous utilisez le mode de mise à jour Auto de la version de l'environnement d'exécution, ou si vous utilisez la version `$LATEST`, vous pouvez rétablir la version de votre environnement d'exécution en

utilisant le mode Manual (Manuel). Pour la version de la fonction que vous voulez rétablir, définissez le mode de mise à jour de la version de l'environnement d'exécution sur Manual (Manuel) et indiquez l'ARN de la version précédente. Pour plus d'informations sur la recherche de l'ARN de la version de l'environnement d'exécution précédente, consultez Identification des changements de version de l'environnement d'exécution Lambda.

> **Note**
>
> Si la version `$LATEST` de votre fonction est configurée pour utiliser le mode Manual (Manuel), vous ne pouvez pas modifier l'architecture du processeur ou la version de l'environnement d'exécution que votre fonction utilise. Pour effectuer ces modifications, vous devez passer en mode Auto ou Function update (Mise à jour de fonction).

Rétablissement d'une version de l'environnement d'exécution à l'aide des versions de fonction publiées

Les versions de fonction publiées sont un instantané immuable du code et de la configuration de la fonction `$LATEST` au moment où vous les avez créées. En mode Auto, Lambda met automatiquement à jour la version de l'environnement d'exécution des versions de fonctions publiées pendant la phase deux du déploiement de la version de l'environnement d'exécution. En mode Function update (Mise à jour de fonction), Lambda ne met pas à jour la version de l'environnement d'exécution des versions de fonctions publiées.

Les versions de fonctions publiées utilisant le mode Function update (Mise à jour de fonction) créent donc un instantané statique du code de la fonction, de la configuration et de la version de l'environnement d'exécution. En utilisant le mode Function update (Mise à jour de fonction) avec les versions de fonctions, vous pouvez synchroniser les mises à jour de l'environnement d'exécution avec vos déploiements. Vous pouvez également coordonner le rétablissement des versions de code, de configuration et de l'environnement d'exécution en redirigeant le trafic vers une version de fonction publiée antérieurement.

Vous pouvez intégrer cette approche à votre intégration continue et à votre livraison continue (CI/CD) pour une annulation entièrement automatique dans les rares cas d'incompatibilité des mises à jour d'exécution. Lorsque vous utilisez cette approche, vous devez mettre à jour votre fonction régulièrement et publier de nouvelles versions de la fonction pour récupérer les dernières mises à jour de l'exécution. Pour plus d'informations, consultez Comprendre le modèle de responsabilité partagée pour la gestion des environnements d'exécution Lambda.

Identification des changements de version de l'environnement d'exécution Lambda

Le numéro de version d'exécution et l'ARN sont enregistrés dans la ligne de `INIT_START` journal, que Lambda envoie à CloudWatch Logs chaque fois qu'il crée un nouvel environnement d'exécution. Étant donné que l'environnement d'exécution utilise la même exécution pour tous les invocations de fonction, Lambda émet la ligne de journal `INIT_START` uniquement lorsqu'il exécute la phase init. Lambda n'émet pas cette ligne de journal pour chaque invocation de fonction. Lambda envoie la ligne de journal à CloudWatch Logs, mais elle n'est pas visible dans la console.

> **Note**
>
> Les numéros de version des environnements d'exécution ne sont pas toujours séquentiels. Par exemple, la version 42 peut être suivie de la version 45.

Example Exemple de ligne de journal INIT_START

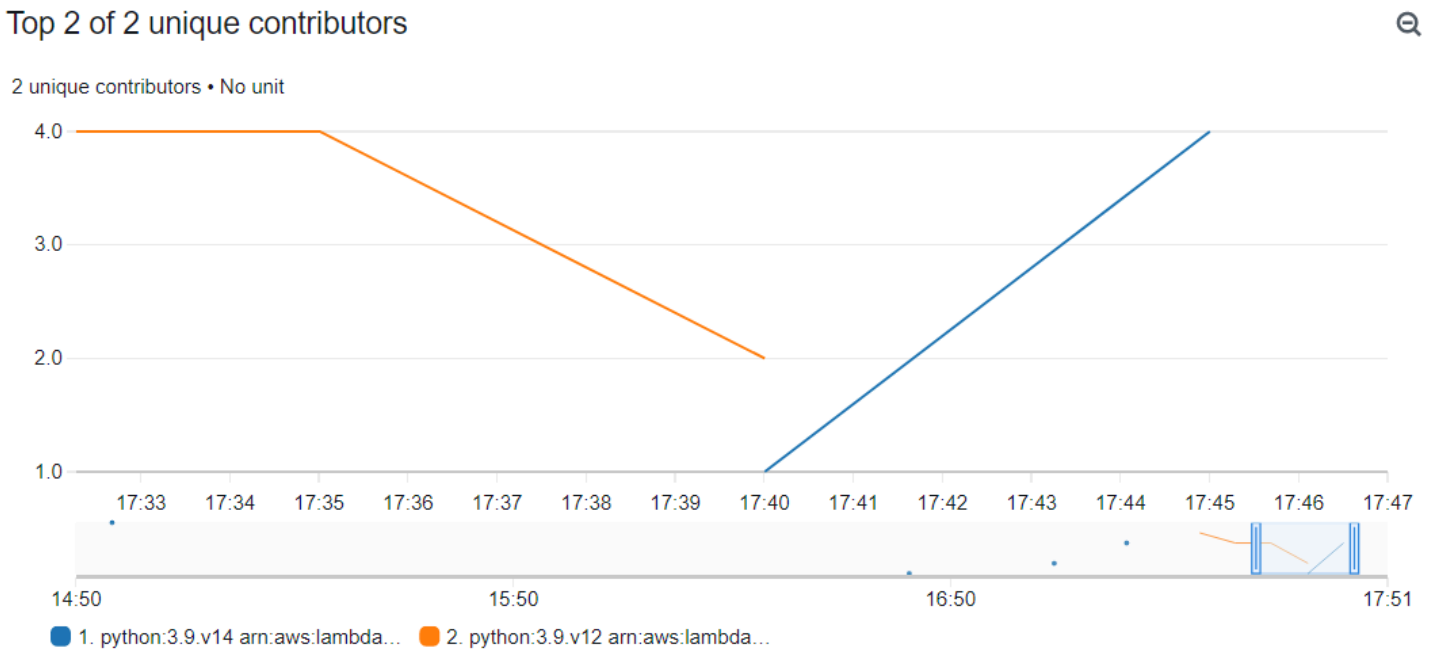
```
INIT_START Runtime Version: python:3.13.v14    Runtime Version ARN: arn:aws:lambda:eu-
south-1::runtime:7b620fc2e66107a1046b140b9d320295811af3ad5d4c6a011fad1fa65127e9e6I
```

Plutôt que de travailler directement avec les journaux, vous pouvez utiliser Amazon CloudWatch Contributor Insights pour identifier les transitions entre les versions d'exécution. La règle suivante compte les versions de l'environnement d'exécution distinctes de chaque ligne de journal `INIT_START`. Pour utiliser la règle, remplacez l'exemple de nom de groupe de journaux `/aws/lambda/*` par le préfixe approprié pour votre fonction ou groupe de fonctions.

```
{
  "Schema": {
    "Name": "CloudWatchLogRule",
    "Version": 1
  },
  "AggregateOn": "Count",
  "Contribution": {
    "Filters": [
      {
        "Match": "eventType",
        "In": [
          "INIT_START"
        ]
      }
```

```
    ],
    "Keys": [
      "runtimeVersion",
      "runtimeVersionArn"
    ]
  },
  "LogFormat": "CLF",
  "LogGroupNames": [
    "/aws/lambda/*"
  ],
  "Fields": {
    "1": "eventType",
    "4": "runtimeVersion",
    "8": "runtimeVersionArn"
  }
}
```

Le rapport CloudWatch Contributor Insights suivant montre un exemple de transition de version d'exécution tel qu'illustré par la règle précédente. La ligne orange indique l'initialisation de l'environnement d'exécution pour la version d'exécution précédente (python:3.13.v12), et la ligne bleue montre l'initialisation de l'environnement d'exécution pour la nouvelle version d'exécution (python:3.13.v14).



Comprendre le modèle de responsabilité partagée pour la gestion des environnements d'exécution Lambda

Lambda est responsable de la conservation et de la publication des mises à jour de sécurité pour tous les environnements d'exécution gérés et les images de conteneurs pris en charge. La responsabilité de mettre à jour les fonctions d'événement existantes pour utiliser la dernière version d'exécution varie en fonction du mode de mise à jour d'exécution que vous utilisez.

Lambda est responsable de l'application des mises à jour de l'environnement d'exécution à toutes les fonctions configurées pour utiliser le mode de mise à jour Auto.

Pour les fonctions configurées avec le mode de mise à jour d'exécution Function update (Mise à jour de fonction), vous êtes responsable de la mise à jour régulière de votre fonction. Lambda est responsable de l'application des mises à jour de l'environnement d'exécution lorsque vous effectuez ces mises à jour. Si vous ne mettez pas à jour votre fonction, Lambda ne met pas à jour l'environnement d'exécution. Si vous ne mettez pas régulièrement à jour votre fonction, nous vous recommandons vivement de la configurer pour les mises à jour automatiques de l'environnement d'exécution afin qu'elle continue à recevoir les mises à jour de sécurité.

Pour les fonctions configurées pour utiliser le mode de mise à jour Manual (Manuel), vous êtes responsable de la mise à jour de votre fonction pour utiliser la dernière version de l'environnement d'exécution. Nous vous recommandons vivement d'utiliser ce mode uniquement pour rétablir la version de l'environnement d'exécution à titre de mesure d'atténuation temporaire dans le cas rare d'une incompatibilité de mise à jour. Nous vous recommandons également de passer en mode Auto le plus rapidement possible afin de minimiser le temps pendant lequel vos fonctions ne sont pas corrigées.

Si vous utilisez des images de conteneur pour déployer vos fonctions, Lambda est responsable de la publication des images de base mises à jour. Dans ce cas, vous êtes responsable de la recréation de l'image de conteneur de votre fonction à partir de la dernière image de base et du redéploiement de l'image de conteneur.

Ceci est résumé dans le tableau suivant :

Mode de déploiement	Responsabilité de Lambda	Responsabilité du client
Environnement	Publiez de nouvelles versions de l'environnement d'exécuti	Rétablissez une version de l'environnement d'exécution précédente dans le cas rare d'un

Mode de déploiement	Responsabilité de Lambda	Responsabilité du client
d'exécution géré, mode Auto	on contenant les derniers correctifs. Appliquez les correctifs de l'environnement d'exécution aux fonctions existantes.	problème de compatibilité de mise à jour de l'environnement d'exécution. Suivez les meilleures pratiques de rétrocompatibilité.
Environnement d'exécution géré, mode Function update (Mise à jour de fonction)	Publiez de nouvelles versions de l'environnement d'exécution contenant les derniers correctifs.	Mettez régulièrement à jour les fonctions afin de bénéficier de la dernière version de l'environnement d'exécution. Passez une fonction en mode Auto lorsque vous ne la mettez pas régulièrement à jour. Rétablissez une version de l'environnement d'exécution précédente dans le cas rare d'un problème de compatibilité de mise à jour de l'environnement d'exécution. Suivez les meilleures pratiques de rétrocompatibilité.
Environnement d'exécution géré, mode Manual (Manuel)	Publiez de nouvelles versions de l'environnement d'exécution contenant les derniers correctifs.	Utilisez ce mode uniquement pour restaurer temporairement l'environnement d'exécution dans le cas rare d'un problème de compatibilité de mise à jour. Passez les fonctions en mode Auto ou Function update (Mise à jour de fonction) et la dernière version de l'environnement d'exécution dès que possible.
Image de conteneur	Publiez de nouvelles images de conteneur contenant les derniers correctifs.	Redéployez régulièrement les fonctions en utilisant la dernière image de base du conteneur pour bénéficier des derniers correctifs.

Pour plus d'informations sur le partage des responsabilités avec AWS, consultez le modèle de responsabilité partagée.

Contrôle des autorisations de mise à jour de l’environnement d’exécution Lambda pour les applications hautement conformes

Pour répondre aux exigences de correctifs, les clients Lambda s’appuient généralement sur des mises à jour automatiques de l’environnement d’exécution. Si votre application est soumise à des exigences strictes en matière de fraîcheur des correctifs, vous souhaiterez peut-être limiter l'utilisation des versions d'exécution antérieures. Vous pouvez restreindre les contrôles de gestion d'exécution de Lambda en utilisant Gestion des identités et des accès AWS (IAM) pour refuser aux utilisateurs de votre AWS compte l'accès à l'opération d'PutRuntimeManagementConfigAPI. Cette opération permet de choisir le mode de mise à jour d'exécution pour une fonction d'événement.

En refusant l’accès à cette opération, toutes les fonctions passent par défaut au mode Auto. Vous pouvez appliquer cette restriction à l’échelle de votre organisation en utilisant des politiques de contrôle des services (SCP). Si vous devez rétablir une fonction à une version de l’environnement d’exécution antérieure, vous pouvez accorder une exception de politique au cas par cas.

Récupérez des données sur les fonctions d'événement Lambda qui utilisent un environnement d'exécution obsolète

Lorsqu'un environnement d'exécution Lambda est sur le point de devenir obsolète, Lambda vous avertit par e-mail et vous envoie des notifications dans le et. Tableau de bord Health Trusted Advisor Ces e-mails et notifications répertorient les versions $LATEST des fonctions utilisant l'environnement d'exécution. Pour répertorier toutes les versions de vos fonctions d'événement qui utilisent un environnement d'exécution particulier, vous pouvez utiliser le AWS Command Line Interface (AWS CLI) ou l'un des AWS SDK.

Si un grand nombre de fonctions utilisent un environnement d'exécution destiné à être obsolète, vous pouvez également utiliser les AWS SDK AWS CLI ou pour vous aider à prioriser les mises à jour de vos fonctions les plus fréquemment invoquées.

Reportez-vous aux sections suivantes pour savoir comment utiliser les AWS SDK AWS CLI et pour collecter des données sur les fonctions d'événement qui utilisent un environnement d'exécution particulier.

Liste des versions de fonctions qui utilisent un environnement d'exécution particulier

Pour répertorier toutes les versions de vos fonctions d'événement Lambda qui utilisent un environnement d'exécution spécifique, exécutez la commande suivante AWS CLI . Cette commande ne renvoie pas les fonctions Web Lambda. `RUNTIME_IDENTIFIER`Remplacez-le par le nom du moteur d'exécution qui est obsolète et choisissez le vôtre. Région AWS Pour répertorier uniquement les versions de fonction $LATEST, omettez `--function-version ALL` dans la commande.

```
aws lambda list-functions --function-version ALL --region us-east-1 --output text --
query "Functions[?Runtime=='RUNTIME_IDENTIFIER'].FunctionArn"
```

> **Tip**
>
> L'exemple de commande répertorie les fonctions d'une `us-east-1` région en particulier. Compte AWS Vous devrez répéter cette commande pour chaque région dans laquelle votre compte possède des fonctions et pour chacune de vos Comptes AWS.

Vous pouvez également répertorier les fonctions d'événement qui utilisent un environnement d'exécution particulier à l'aide de l'un des AWS SDK. L'exemple de code suivant utilise l' AWS SDK pour JavaScript V3 et l' AWS SDK pour Python (Boto3) pour renvoyer une liste des ARN de fonctions

utilisant un environnement d'exécution particulier. L'exemple de code renvoie également le groupe de CloudWatch journaux pour chacune des fonctions répertoriées. Vous pouvez utiliser ce groupe de journaux pour trouver la date de la dernière invocation de la fonction. Consultez la section the section called "Identification des fonctions les plus fréquemment et les plus récemment invoquées" suivante pour plus d'informations.

Node.js

Example JavaScript code pour répertorier les fonctions utilisant un environnement d'exécution particulier

```
import { LambdaClient, ListFunctionsCommand } from "@aws-sdk/client-lambda";
const lambdaClient = new LambdaClient();

const command = new ListFunctionsCommand({
    FunctionVersion: "ALL",
    MaxItems: 50
});
const response = await lambdaClient.send(command);

for (const f of response.Functions){
    if (f.Runtime == '<your_runtime>'){ // Use the runtime id, e.g. 'nodejs24.x' or
 'python3.14'
        console.log(f.FunctionArn);
        // get the CloudWatch log group of the function to
        // use later for finding the last invocation date
        console.log(f.LoggingConfig.LogGroup);
    }
}
// If your account has more functions than the specified
// MaxItems, use the returned pagination token in the
// next request with the 'Marker' parameter
if ('NextMarker' in response){
    let paginationToken = response.NextMarker;
  }
```

Python

Example Code Python pour répertorier les fonctions utilisant un environnement d'exécution particulier

```
import boto3
```

```
from botocore.exceptions import ClientError

def list_lambda_functions(target_runtime):

    lambda_client = boto3.client('lambda')

    response = lambda_client.list_functions(
        FunctionVersion='ALL',
        MaxItems=50
    )
    if not response['Functions']:
            print("No Lambda functions found")
    else:
        for function in response['Functions']:
            if function['PackageType']=='Zip' and function['Runtime'] ==
 target_runtime:
                print(function['FunctionArn'])
                # Print the CloudWatch log group of the function
                # to use later for finding last invocation date
                print(function['LoggingConfig']['LogGroup'])

    if 'NextMarker' in response:
       pagination_token = response['NextMarker']

if __name__ == "__main__":
    # Replace python3.12 with the appropriate runtime ID for your Lambda functions
    list_lambda_functions('python3.12')
```

Pour en savoir plus sur l'utilisation d'un AWS SDK pour répertorier vos fonctions à l'aide de l'ListFunctionsaction, consultez la documentation du SDK correspondant à votre langage de programmation préféré.

Vous pouvez également utiliser la fonctionnalité de requêtes AWS Config avancées pour répertorier toutes vos fonctions d'événement Lambda qui utilisent un environnement d'exécution affecté. AWS Config ne renvoie pas les fonctions Web Lambda. Cette requête renvoie uniquement les versions $LATEST de la fonction, mais vous pouvez agréger les requêtes pour répertorier les fonctions dans toutes les régions et plusieurs Comptes AWS avec une seule commande. Pour en savoir plus, consultez la section Interrogation de l'état de configuration actuel des AWS Auto Scaling ressources dans le guide du AWS Config développeur.

Identification des fonctions les plus fréquemment et les plus récemment invoquées

Si vous utilisez Compte AWS des fonctions qui utilisent un environnement d'exécution destiné à être obsolète, vous souhaiterez peut-être donner la priorité à la mise à jour des fonctions fréquemment invoquées ou des fonctions qui ont été invoquées récemment.

Si vous ne disposez que de quelques fonctions, vous pouvez utiliser la console CloudWatch Logs pour recueillir ces informations en consultant les flux de journaux de vos fonctions. Voir Afficher les données de journal envoyées à CloudWatch Logs pour plus d'informations.

Pour connaître le nombre d'appels de fonctions récents, vous pouvez également utiliser les informations de CloudWatch métriques affichées dans la console Lambda. Pour afficher ces informations, procédez comme suit :

1. Ouvrez la page Event Functions de la console Lambda.
2. Sélectionnez la fonction dont vous souhaitez consulter les statistiques d'invocation.
3. Choisissez l'onglet Surveiller.
4. Définissez la période pendant laquelle vous souhaitez consulter les statistiques à l'aide du sélecteur de plage de dates. Les invocations récentes sont affichées dans le volet Invocations.

Pour les comptes dotés d'un plus grand nombre de fonctions, il peut être plus efficace de collecter ces données par programmation à l'aide du SDK AWS CLI ou de l'un des AWS SDK à l'aide des actions DescribeLogStreamset GetMetricStatisticsde l'API.

Les exemples suivants fournissent des extraits de code utilisant la V3 AWS SDK pour JavaScript et le AWS SDK pour Python (Boto3) pour identifier la date du dernier appel pour une fonction particulière et pour déterminer le nombre d'appels pour une fonction particulière au cours des 14 derniers jours.

Node.js

Example JavaScript code pour trouver l'heure du dernier appel d'une fonction

```
import { CloudWatchLogsClient, DescribeLogStreamsCommand } from "@aws-sdk/client-
cloudwatch-logs";
const cloudWatchLogsClient = new CloudWatchLogsClient();
const command = new DescribeLogStreamsCommand({
    logGroupName: '<your_log_group_name>',
    orderBy: 'LastEventTime',
    descending: true,
```

```
    limit: 1
});
try {
    const response = await cloudWatchLogsClient.send(command);
    const lastEventTimestamp = response.logStreams.length > 0 ?
        response.logStreams[0].lastEventTimestamp : null;
    // Convert the UNIX timestamp to a human-readable format for display
    const date = new Date(lastEventTimestamp).toLocaleDateString();
    const time = new Date(lastEventTimestamp).toLocaleTimeString();
    console.log(`${date} ${time}`);

} catch (e){
    console.error('Log group not found.')
}
```

Python

Example Code Python pour trouver l'heure de la dernière invocation d'une fonction

```
import boto3
from datetime import datetime

cloudwatch_logs_client  = boto3.client('logs')

response = cloudwatch_logs_client.describe_log_streams(
    logGroupName='<your_log_group_name>',
    orderBy='LastEventTime',
    descending=True,
    limit=1
)

try:
    if len(response['logStreams']) > 0:
        last_event_timestamp = response['logStreams'][0]['lastEventTimestamp']
        print(datetime.fromtimestamp(last_event_timestamp/1000)) # Convert timestamp
 from ms to seconds
    else:
        last_event_timestamp = None
except:
    print('Log group not found')
```

> **Tip**
>
> Vous pouvez trouver le nom du groupe de journaux de votre fonction à l'aide de l'opération ListFunctionsAPI. Consultez le code dans the section called “Liste des versions de fonctions qui utilisent un environnement d’exécution particulier” pour obtenir un exemple montrant la façon de procéder.

Node.js

Example JavaScript code pour trouver le nombre d'invocations au cours des 14 derniers jours

```
import { CloudWatchClient, GetMetricStatisticsCommand } from "@aws-sdk/client-
cloudwatch";
const cloudWatchClient = new CloudWatchClient();
const command = new GetMetricStatisticsCommand({
    Namespace: 'AWS/Lambda',
    MetricName: 'Invocations',
    StartTime: new Date(Date.now()-86400*1000*14), // 14 days ago
    EndTime: new Date(Date.now()),
    Period: 86400 * 14, // 14 days.
    Statistics: ['Sum'],
    Dimensions: [{
        Name: 'FunctionName',
        Value: '<your_function_name>'
    }]
});
const response = await cloudWatchClient.send(command);
const invokesInLast14Days = response.Datapoints.length > 0 ?
    response.Datapoints[0].Sum : 0;

console.log('Number of invocations: ' + invokesInLast14Days);
```

Python

Example Code Python pour trouver le nombre d’invocations au cours des 14 derniers jours

```
import boto3
from datetime import datetime, timedelta

cloudwatch_client = boto3.client('cloudwatch')
```

```
response = cloudwatch_client.get_metric_statistics(
    Namespace='AWS/Lambda',
    MetricName='Invocations',
    Dimensions=[
        {
            'Name': 'FunctionName',
            'Value': '<your_function_name>'
        },
    ],
    StartTime=datetime.now() - timedelta(days=14),
    EndTime=datetime.now(),
    Period=86400 * 14, # 14 days
    Statistics=[
        'Sum'
    ]
)

if len(response['Datapoints']) > 0:
    invokes_in_last_14_days = int(response['Datapoints'][0]['Sum'])
else:
    invokes_in_last_14_days = 0

print(f'Number of invocations: {invokes_in_last_14_days}')
```

Modification de l’environnement d’exécution

Vous pouvez utiliser des extensions internes pour modifier le processus de runtime. Les extensions internes ne sont pas des processus séparés. Elles s’exécutent dans le cadre du processus du runtime.

Lambda fournit des variables d’environnement spécifiques du langage, que vous pouvez définir pour ajouter des options et des outils au runtime. Lambda intègre également des scripts encapsuleurs qui lui permettent de déléguer le démarrage du runtime à votre script. Vous pouvez créer un script encapsuleur pour personnaliser le comportement de démarrage du runtime.

Language-specific variables d'environnement

Lambda prend en charge des méthodes de configuration pour permettre le pré-chargement de code lors de l’initialisation de la fonction via les variables d’environnement spécifiques du langage suivantes :

- `JAVA_TOOL_OPTIONS` : sur Java, Lambda prend en charge cette variable d’environnement pour définir des variables de ligne de commande supplémentaires dans Lambda. Cette variable d’environnement vous permet de spécifier l’initialisation des outils, en particulier le lancement d’agents de langage de programmation natifs ou Java à l’aide des options `agentlib` ou `javaagent`. Pour plus d’informations, veuillez consulter la rubrique Variables d’environnement `JAVA_TOOL_OPTIONS`.
- `NODE_OPTIONS`— Disponible dans les environnements d'Node.js exécution.
- `DOTNET_STARTUP_HOOKS` – Sur .NET Core 3.1 et versions ultérieures, cette variable d’environnement précise le chemin d’accès d’un assembly (dll) que Lambda peut utiliser.

L’utilisation de variables d’environnement spécifiques à un langage est la méthode privilégiée pour définir les propriétés de démarrage.

Scripts encapsuleurs

Vous pouvez créer un script wrapper pour personnaliser le comportement de démarrage de votre fonction d'événement Lambda au moment de l'exécution. Avec un script wrapper, vous pouvez définir des paramètres de configuration qui ne peuvent pas être définis par le biais de variables d'environnement spécifiques au langage.

> **Note**
>
> Les invocations peuvent échouer si le script wrapper ne démarre pas correctement le processus d'exécution.

Les scripts encapsulateurs sont pris en charge sur tous les environnements d'exécution Lambda natifs. Les scripts Wrapper ne sont pas pris en charge sur OS-only runtimes (famille d'environnements d'exécution `provided`).

Lorsque vous utilisez un script encapsuleur pour votre fonction, Lambda démarre le runtime en utilisant votre script. Lambda envoie à votre script le chemin d'accès de l'interpréteur et tous les arguments d'origine pour le démarrage du runtime standard. Votre script peut étendre ou transformer le comportement de démarrage du programme. Par exemple, le script peut injecter et modifier des arguments, définir des variables d'environnement ou capturer des métriques, des erreurs et d'autres informations de diagnostic.

Vous spécifiez le script en définissant la valeur de la variable d'environnement `AWS_LAMBDA_EXEC_WRAPPER` comme étant le chemin vers le système de fichiers d'un fichier binaire ou d'un script exécutable.

Exemple : Créer et utiliser un script encapsuleur en tant que couche Lambda

Dans l'exemple suivant, vous créez un script encapsuleur pour démarrer l'interpréteur Python avec l'option `-X importtime`. Lorsque vous exécutez la fonction, Lambda génère une entrée de journal pour indiquer la durée de chaque importation.

Pour créer et utiliser un script encapsuleur en tant que couche

1. Créez un répertoire pour la couche :

   ```
   mkdir -p python-wrapper-layer/bin
   cd python-wrapper-layer/bin
   ```

2. Dans le répertoire `bin`, collez le code suivant dans un nouveau fichier nommé `importtime_wrapper`. Il s'agit du script encapsuleur.

   ```
   #!/bin/bash

   # the path to the interpreter and all of the originally intended arguments
   ```

```
args=("$@")

# the extra options to pass to the interpreter
extra_args=("-X" "importtime")

# insert the extra options
args=("${args[@]:0:$#-1}" "${extra_args[@]}" "${args[@]: -1}")

# start the runtime with the extra options
exec "${args[@]}"
```

3. Fournissez au script des autorisations d'exécution :

```
chmod +x importtime_wrapper
```

4. Créez un fichier .zip pour la couche :

```
cd ..
zip -r ../python-wrapper-layer.zip .
```

5. Vérifiez que votre fichier .zip possède la structure de répertoire suivante :

```
python-wrapper-layer.zip
# bin
    # importtime_wrapper
```

6. Créez une couche à l'aide du package .zip.
7. Créez une fonction d'événement à l'aide de la console Lambda.
   a. Ouvrez la console Lambda.
   b. Choisissez Create Event Function.
   c. Indiquez un Function name (Nom de fonction).
   d. Pour Environnement d'exécution, choisissez le dernier environnement d'exécution Python pris en charge (Dernier pris en charge).
   e. Choisissez Create Event Function.
8. Ajoutez la couche à votre fonction.
   a. Choisissez votre fonction, puis choisissez l'onglet Code s'il n'est pas déjà sélectionné.
   b. Faites défiler jusqu'à la section Couches, puis choisissez Ajouter une couche.

c. Pour Source de la couche, sélectionnez Couches personnalisées, puis choisissez votre couche dans la liste déroulante Couches personnalisées.

d. Pour Version, choisissez 1.

e. Choisissez Ajouter.

9. Ajoutez la variable d'environnement encapsuleur.

a. Choisissez Configuration, puis Variables d'environnement.

b. Sous Variables d'environnement, choisissez Modifier.

c. Choisissez Ajouter une variable d'environnement.

d. Pour Clé, entrez `AWS_LAMBDA_EXEC_WRAPPER`.

e. Dans Valeur, saisissez `/opt/bin/importtime_wrapper` (`/opt/` + la structure de dossiers de votre couche .zip).

f. Cliquez sur Enregistrer.

10. Testez le script encapsuleur.

a. Choisissez l'onglet Test.

b. Sous Événement de test, choisissez Tester. Il n'est pas nécessaire de créer un événement de test, l'événement par défaut fonctionne.

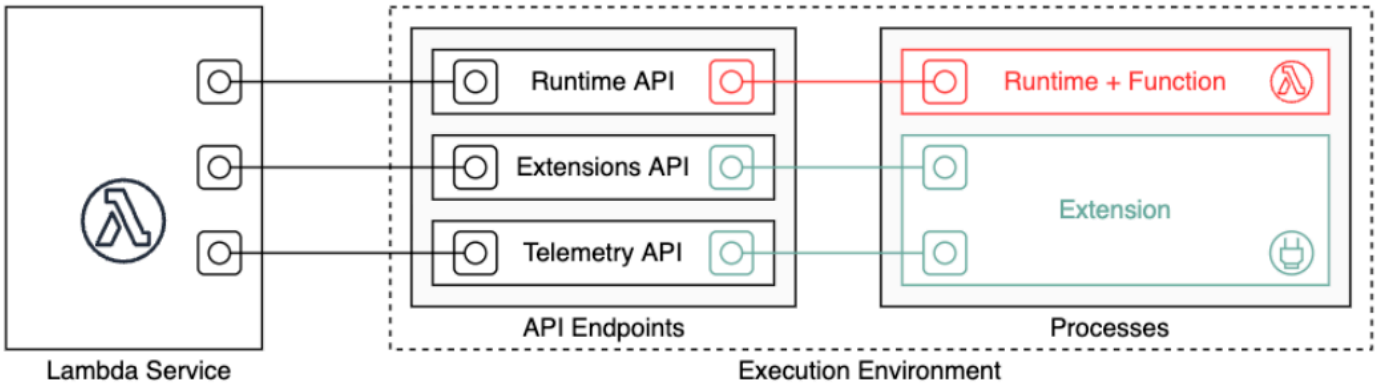
c. Faites défiler la page jusqu'à Sortie de journal. Votre script encapsuleur ayant lancé l'interpréteur Python avec l'option `-X importtime`, les journaux indiquent le temps requis pour chaque importation. Exemples :

```
532 |           collections
import time:        63 |         63 |           _functools
import time:      1053 |       3646 |         functools
import time:      2163 |       7499 |       enum
import time:       100 |        100 |         _sre
import time:       446 |        446 |           re._constants
import time:       691 |       1136 |         re._parser
import time:       378 |        378 |         re._casefix
import time:       670 |       2283 |       re._compiler
import time:       416 |        416 |       copyreg
```

Utilisation de l'API de l'environnement d'exécution Lambda pour des environnements d'exécution personnalisés

AWS Lambda fournit une API HTTP pour les exécutions personnalisées des fonctions d'événement Lambda afin de recevoir les événements d'invocation de Lambda et de renvoyer les données de réponse dans l'environnement d'exécution Lambda. Cette section contient la référence de l'API de l'environnement d'exécution Lambda.

> **Les instances gérées Lambda prennent en charge les demandes simultanées**
>
> Les instances gérées Lambda utilisent la même API d'exécution que les fonctions qui utilisent le fournisseur de capacité par défaut Lambda. La principale différence réside dans le fait que les instances gérées peuvent accepter `/next` des `/response` demandes simultanées et jusqu'à la `AWS_LAMBDA_MAX_CONCURRENCY` limite configurée. Cela permet de traiter plusieurs appels simultanément au sein d'un même environnement d'exécution. Pour plus d'informations sur les instances gérées, consultezComprendre l'environnement d'exécution des instances gérées Lambda.



La spécification OpenAPI pour la version d'API de l'exécution 2018-06-01 est disponible dans runtime-api.zip

Pour créer une URL de requête d'API, les exécutions obtiennent le point de terminaison de l'API à partir de la variable d'environnement `AWS_LAMBDA_RUNTIME_API` et ajoutent la version de l'API ainsi que le chemin d'accès de ressource souhaité.

Example Demande

```
curl "http://${AWS_LAMBDA_RUNTIME_API}/2018-06-01/runtime/invocation/next"
```

Méthodes d'API

- Invocation suivante
- Réponse d'invocation
- Erreur d'initialisation
- Erreur d'invocation
- After-Restore (applicable uniquement pour SnapStart)
- Erreur de restauration (applicable uniquement pour SnapStart)

Invocation suivante

Chemin – `/runtime/invocation/next`

Méthode – GET

L'exécution envoie ce message à Lambda pour demander un événement d'invocation. Le corps de la réponse contient la charge utile provenant de l'invocation, qui est un document JSON contenant les données d'événements du déclencheur de la fonction. Les en-têtes de la réponse contiennent des données supplémentaires sur l'invocation.

En-têtes de réponse

- `Lambda-Runtime-Aws-Request-Id`— L'événement qui a déclenché l'invocation de la fonction. Les sources d'événements fournissent des identifiants de demande, ou Lambda les génère automatiquement lors de l'ingestion. Un identifiant de demande unique peut entraîner plusieurs tentatives d'invocation. Utilisez-le dans le chemin de l'URL lors de l'envoi de la réponse ou de l'erreur.

  Par exemple : `8476a536-e9f4-11e8-9739-2dfe598c3fcd`.
- `Lambda-Runtime-Deadline-Ms` – Date à laquelle la fonction expire, exprimée en millisecondes au format horaire Unix.

  Par exemple : `1542409706888`.

- `Lambda-Runtime-Invoked-Function-Arn` – ARN de la fonction Lambda, de la version ou de l'alias spécifiés dans l'invocation.

  Par exemple : `arn:aws:lambda:us-east-2:123456789012:function:custom-runtime`.

- `Lambda-Runtime-Trace-Id` – En-tête de suivi AWS X-Ray.

  Par exemple : `Root=1-5bef4de7-ad49b0e87f6ef6c87fc2e700;Parent=9a9197af755a6419;Sampled=1`.

- `Lambda-Runtime-Client-Context`— Pour les appels depuis le SDK AWS mobile, les données relatives à l'application client et à l'appareil.
- `Lambda-Runtime-Cognito-Identity`— Pour les appels depuis le SDK AWS mobile, les données relatives au fournisseur d'identité Amazon Cognito.
- `Lambda-Runtime-Invocation-Id`— Un identifiant unique pour cette tentative d'invocation.

Ne définissez pas de délai d'expiration pour la demande `GET`, car la réponse peut être retardée. Entre le moment où Lambda démarre le moteur d'exécution et le moment où celui-ci doit renvoyer un événement, le processus d'exécution peut être gelé pendant plusieurs secondes.

Un ID de demande (`Lambda-Runtime-Aws-Request-Id`) identifie un événement unique. Les identifiants de demande sont fournis par des sources d'événements ou générés automatiquement par Lambda lors de l'ingestion. Utilisez l'ID de demande indiqué dans le chemin de l'URL lors de l'envoi de la réponse ou de l'erreur.

Un ID d'appel (`Lambda-Runtime-Invocation-Id`) représente une tentative d'invocation unique pour un événement. Un identifiant de demande unique peut entraîner plusieurs tentatives d'invocation, chacune ayant son propre identifiant d'appel unique. Lambda utilise chaque ID d'appel une seule fois et ne le réutilise jamais. Réactivez cette valeur `/response` et `/error` appelez. L'en-tête est facultatif pour des raisons de rétrocompatibilité avec les environnements d'exécution existants ; son omission ne déclenche pas de rejet. Lambda rejette uniquement with `400 InvalidInvocationId` lorsque l'en-tête est présent mais que sa valeur ne correspond pas à l'invocation active.

L'en-tête de suivi contient l'ID de suivi, l'ID parent et la décision d'échantillonnage. Si la demande est échantillonnée, elle a été échantillonnée par Lambda ou un service en amont. Le runtime doit définir l'`_X_AMZN_TRACE_ID` avec la valeur de l'en-tête. Le X-Ray SDK le lit pour obtenir les identifiants et déterminer s'il convient de suivre la demande.

Réponse d'invocation

Chemin – `/runtime/invocation/AwsRequestId/response`

Méthode – POST

Une fois l'exécution de la fonction terminée, le runtime envoie une réponse à l'invocation à Lambda. Pour les invocations synchrones, Lambda envoie la réponse au client.

En-têtes de demandes

`Lambda-Runtime-Invocation-Id`— Renvoie la valeur reçue de`/next`. Lambda rejette la demande `400 InvalidInvocationId` si la valeur ne correspond pas à l'invocation active.

Example demande d'opération réussie

```
REQUEST_ID=156cb537-e2d4-11e8-9b34-d36013741fb9
INVOCATION_ID=<value from Lambda-Runtime-Invocation-Id response header>
curl "http://${AWS_LAMBDA_RUNTIME_API}/2018-06-01/runtime/invocation/$REQUEST_ID/
response"  -d "SUCCESS" --header "Lambda-Runtime-Invocation-Id: $INVOCATION_ID"
```

Erreur d'initialisation

Si la fonction renvoie une erreur ou si le runtime rencontre une erreur lors de l'initialisation, le runtime utilise cette méthode pour signaler l'erreur à Lambda.

Chemin – `/runtime/init/error`

Méthode – POST

En-têtes

`Lambda-Runtime-Function-Error-Type` : le type d'erreur que l'exécution a rencontré. Cet en-tête est facultatif. Lambda accepte n'importe quelle valeur de chaîne ; nous vous recommandons d'utiliser le format `<Category.Reason>` dans lequel Category est `Runtime` ou `Function` et Reason commence par une lettre majuscule. Par exemple :

- `Runtime.NoSuchHandler`
- `Runtime.APIKeyNotFound`
- `Runtime.ConfigInvalid`
- `Runtime.BeforeSnapshotError`(pour SnapStart)

- `Runtime.UnknownReason`

Les valeurs qui ne correspondent pas à ce modèle sont normalisées à `Runtime.Unknown` ou`Function.Unknown`.

Paramètres de corps

`ErrorRequest` : informations sur l'erreur. Requis : non.

Ce champ est un objet JSON avec la structure suivante :

```
{
      errorMessage: string (text description of the error),
      errorType: string,
      stackTrace: array of strings
}
```

Notez que Lambda accepte n'importe quelle valeur pour `errorType`.

L'exemple suivant montre un message d'erreur de fonction Lambda indiquant que la fonction n'a pas pu analyser les données d'événement fournies dans l'invocation.

Example Erreur de fonction

```
{
      "errorMessage" : "Error parsing event data.",
      "errorType" : "InvalidEventDataException",
      "stackTrace": [ ]
}
```

Paramètres du corps de la réponse

- `StatusResponse` – String. Informations d'état, envoyées avec les codes de réponse 202.
- `ErrorResponse`— Informations d'erreur supplémentaires, envoyées avec les codes de réponse d'erreur. ErrorResponse contient un type d'erreur et un message d'erreur.

Codes de réponse

- 202 – Accepté
- 403 – Interdit

- 500 — Erreur du conteneur. Non-recoverable état. L'environnement d'exécution doit se terminer rapidement.

Example demande d'erreur d'initialisation

```
ERROR="{\"errorMessage\" : \"Failed to load function.\", \"errorType\" :
 \"InvalidFunctionException\"}"
curl "http://${AWS_LAMBDA_RUNTIME_API}/2018-06-01/runtime/init/error" -d "$ERROR" --
header "Lambda-Runtime-Function-Error-Type: Unhandled"
```

Erreur d'invocation

Si la fonction renvoie une erreur ou si le runtime rencontre une erreur, le runtime utilise cette méthode pour signaler l'erreur à Lambda.

Chemin – `/runtime/invocation/AwsRequestId/error`

Méthode – POST

En-têtes

`Lambda-Runtime-Function-Error-Type` – Type d'erreur que l'environnement d'exécution a rencontré. Requis : non.

Cet en-tête se compose d'une valeur de chaîne. Lambda accepte n'importe quelle chaîne, mais nous recommandons le format <category.reason>. Par exemple :

- Runtime.NoSuchHandler
- Runtime.APIKeyNotFound
- Runtime.ConfigInvalid
- Runtime.UnknownReason

`Lambda-Runtime-Invocation-Id`— Renvoie la valeur reçue de`/next`. Lambda rejette la demande `400 InvalidInvocationId` si la valeur ne correspond pas à l'invocation active.

Paramètres de corps

`ErrorRequest` : informations sur l'erreur. Requis : non.

Ce champ est un objet JSON avec la structure suivante :

```
{
      errorMessage: string (text description of the error),
      errorType: string,
      stackTrace: array of strings
}
```

Notez que Lambda accepte n'importe quelle valeur pour `errorType`.

L'exemple suivant montre un message d'erreur de fonction Lambda indiquant que la fonction n'a pas pu analyser les données d'événement fournies dans l'invocation.

Example Erreur de fonction

```
{
      "errorMessage" : "Error parsing event data.",
      "errorType" : "InvalidEventDataException",
      "stackTrace": [ ]
}
```

Paramètres du corps de la réponse

- `StatusResponse` – String. Informations d'état, envoyées avec les codes de réponse 202.
- `ErrorResponse`— Informations d'erreur supplémentaires, envoyées avec les codes de réponse d'erreur. ErrorResponse contient un type d'erreur et un message d'erreur.

Codes de réponse

- 202 – Accepté
- 400 – Demande erronée.
- 403 – Interdit
- 500 — Erreur du conteneur. Non-recoverable état. L'environnement d'exécution doit se terminer rapidement.

Example demande d'erreur

```
REQUEST_ID=156cb537-e2d4-11e8-9b34-d36013741fb9
ERROR="{\"errorMessage\" : \"Error parsing event data.\", \"errorType\" :
 \"InvalidEventDataException\"}"
```

```
curl "http://${AWS_LAMBDA_RUNTIME_API}/2018-06-01/runtime/invocation/$REQUEST_ID/error"
 -d "$ERROR" --header "Lambda-Runtime-Function-Error-Type: Unhandled"
```

After-Restore (applicable uniquement pour SnapStart)

Chemin – `/runtime/restore/next`

Méthode – GET

Une fois les hooks antérieurs à la capture d'écran terminés, le moteur d'exécution appelle. `GET /runtime/restore/next` Il s'agit d'un appel de blocage de type itérateur, similaire à`/runtime/invocation/next`, qui indique à Lambda que le moteur d'exécution est prêt pour la capture instantanée de l'environnement d'exécution. La requête est bloquée jusqu'à ce que Lambda restaure l'environnement d'exécution à partir d'un instantané, puis renvoie une réponse HTTP 200 avec un corps vide.

En-têtes

Aucun en-tête n'est requis.

Codes de réponse

- 200 — Lambda a restauré l'environnement d'exécution. Exécutez les hooks après restauration. Le corps de la réponse est vide.
- 403 — Interdit. L'environnement d'exécution n'est pas dans un état qui l'autorise `/restore/next` (par exemple, le moteur d'exécution a déjà appelé `/invocation/next` ou`/restore/next`).
- 404 — n' SnapStart est pas activé pour cette fonction.
- 500 – Erreur de conteneur. L'environnement d'exécution est dans un état irrécupérable. Quittez le processus d'exécution.

Syntaxe de demande

```
GET /2018-06-01/runtime/restore/next HTTP/1.1
Host: ${AWS_LAMBDA_RUNTIME_API}
```

Syntaxe de réponse

```
HTTP/1.1 200 OK
Content-Length: 0
```

> **Note**
>
> Ne définissez pas de socket côté client ni de délai de lecture pour cette demande d'API Runtime (ou pour toute autre). Il s'agit d'un appel de blocage de type itérateur ; Lambda bloque l'environnement d'exécution pendant que la requête est ouverte. La demande peut rester ouverte pendant toute la durée de vie du snapshot (potentiellement des jours, des semaines ou plus) sans que la connexion ne soit considérée comme inactive par le service Lambda.

Erreur de restauration (applicable uniquement pour SnapStart)

Si un hook après restauration échoue ou si le moteur d'exécution rencontre une erreur lors de la restauration, le moteur d'exécution utilise cette méthode pour signaler l'erreur à Lambda. Lambda échoue à l'invocation en vol et détruit l'environnement d'exécution.

Chemin – `/runtime/restore/error`

Méthode – POST

En-têtes

`Lambda-Runtime-Function-Error-Type` : le type d'erreur que l'exécution a rencontré. Cet en-tête est facultatif. Lambda accepte n'importe quelle valeur de chaîne ; nous vous recommandons d'utiliser le format `<Category.Reason>` dans lequel Category est `Runtime` ou `Function` et Reason commence par une lettre majuscule (par exemple,). `Runtime.AfterRestoreError` Les valeurs qui ne correspondent pas à ce modèle sont normalisées à `Runtime.Unknown` ou`Function.Unknown`.

Codes de réponse

- 202 — Acceptée. Le corps de réponse est`{"status":"OK"}`. Le moteur d'exécution doit quitter le processus.
- 403 — Interdit. L'environnement d'exécution n'est pas dans un état qui l'autorise `/restore/error` (par exemple, `/restore/next` il n'a pas été appelé).
- 404 — n' SnapStart est pas activé pour cette fonction.
- 500 – Erreur de conteneur. L'environnement d'exécution est dans un état irrécupérable. Quittez le processus d'exécution.

Syntaxe de demande

```
POST /2018-06-01/runtime/restore/error HTTP/1.1
Host: ${AWS_LAMBDA_RUNTIME_API}
Lambda-Runtime-Function-Error-Type: Runtime.AfterRestoreError
```

Syntaxe de réponse

```
HTTP/1.1 202 Accepted
Content-Type: application/json

{"status":"OK"}
```

Quand utiliser les environnements d'exécution de Lambda OS-only

Lambda fournit des environnements d'exécution gérés pour Java, Python Node.js, .NET et Ruby. Pour créer des fonctions d'événement Lambda dans un langage de programmation qui n'est pas disponible en tant qu'environnement d'exécution géré, utilisez un environnement d' OS-only exécution (la famille des environnements `provided` d'exécution). Il existe trois principaux cas d'utilisation des OS-only runtimes :

- Compilation native à l'avance (AOT) : des langages tels que Go, Rust, Swift et C++ se compilent nativement en un binaire exécutable, ce qui ne nécessite pas d'environnement d'exécution de langage dédié. Ces langages ont uniquement besoin d'un environnement de système d'exploitation dans lequel le binaire compilé peut s'exécuter. Vous pouvez également utiliser les environnements d' OS-only exécution Lambda pour déployer des fichiers binaires compilés avec .NET Native AOT et Java GraalVM Native Image.

  Vous devez inclure un client d'interface d'exécution. Le client de l'interface d'exécution appelle l'Utilisation de l'API de l'environnement d'exécution Lambda pour des environnements d'exécution personnalisés pour récupérer les invocations de fonction, puis appelle votre gestionnaire de fonctions. Lambda fournit des clients d'interface d'exécution pour Rust, Go, .NET Native AOT, Swift (expérimental) et C++ (expérimental).

  Vous devez compiler votre binaire pour un environnement Linux et pour la même architecture de jeu d'instructions que celle que vous prévoyez d'utiliser pour la fonction (x86_64 ou arm64).
- Third-party runtimes : vous pouvez exécuter des fonctions à l'aide d'environnements d'exécution standard tels que Bref pour PHP.
- Runtimes personnalisés : vous pouvez créer votre propre environnement d'exécution pour une langue ou une version de langue pour laquelle Lambda ne fournit pas d'environnement d'exécution géré, par exemple Node.js 19. Pour plus d'informations, consultez Création d'un environnement d'exécution personnalisé pour AWS Lambda Fonctions événementielles. Il s'agit du cas d'utilisation le moins courant pour les environnements d' OS-only exécution.

Lambda prend en charge les environnements d'exécution suivants : OS-only

Nom	Identifiant	Système d'exploitation	Date d'obsolescence	Créer la fonction de blocage	Mettre à jour la fonction de blocage
OS-only Temps d'exécution	`provided.al2023`	Amazon Linux 2	30 juin 2029	31 juillet 2029	31 août 2029

L'environnement d'exécution Amazon Linux 2023 (`provided.al2023`) offre plusieurs avantages par rapport à Amazon Linux 2, notamment un encombrement de déploiement réduit et des versions mises à jour de bibliothèques telles que `glibc`.

L'environnement d'exécution `provided.al2023` utilise `dnf` comme gestionnaire de packages au lieu de `yum`, qui est le gestionnaire de packages par défaut dans Amazon Linux 2. Pour plus d'informations sur les différences entre `provided.al2023` et`provided.al2`, consultez Présentation du runtime Amazon Linux 2023 AWS Lambda sur le blog AWS Compute.

Création d'un environnement d'exécution personnalisé pour AWS Lambda Fonctions événementielles

Vous pouvez implémenter un AWS Lambda environnement d'exécution dans n'importe quel langage de programmation. Un environnement d'exécution est un programme qui exécute la méthode de gestion d'une fonction d'événement Lambda lorsque la fonction est invoquée. Vous pouvez inclure le runtime dans le package de déploiement de votre fonction ou le distribuer dans une couche. Lorsque vous créez la fonction, choisissez un OS-only environnement d'exécution (la famille `provided` d'environnements d'exécution).

> **Note**
>
> La création d'un environnement d'exécution personnalisé est un cas d'utilisation avancé. Si vous recherchez des informations sur la compilation vers un binaire natif ou sur l'utilisation d'un environnement d'exécution tiers prêt à l'emploi, consultez Quand utiliser les environnements d'exécution de Lambda OS-only.

Pour une présentation détaillée du processus de déploiement d'un environnement d'exécution personnalisé, voir Tutoriel : création d'un environnement d'exécution personnalisé.

Rubriques

- Exigences
- Implémentation du flux de réponses dans un environnement d'exécution personnalisé
- Création d'environnements d'exécution personnalisés pour les instances gérées Lambda

Exigences

Les environnements d'exécution personnalisés doivent effectuer certaines tâches d'initialisation et de traitement. Une exécution exécute le code d'installation de la fonction, lit le nom du gestionnaire à partir d'une variable d'environnement et lit les événements d'invocation à partir de l'API d'exécution Lambda. L'environnement d'exécution transmet les données d'événements au gestionnaire de la fonction, et renvoie la réponse du gestionnaire à Lambda.

Tâches d'initialisation

Les tâches d'initialisation sont exécutées une seule fois par instance de la fonction pour préparer l'environnement à la gestion des invocations.

- Récupérer les paramètres – Lecture des variables d'environnement pour obtenir des détails sur la fonction et l'environnement.
  - `_HANDLER` – Emplacement du gestionnaire, issu de la configuration de la fonction. Le format standard est *`file`*`.`*`method`*, où `file` est le nom du fichier sans extension et `method` est le nom d'une méthode ou fonction qui est définie dans le fichier.
  - `LAMBDA_TASK_ROOT` – Répertoire contenant le code de la fonction.
  - `AWS_LAMBDA_RUNTIME_API` – Hôte et port de l'API d'exécution.

  Pour obtenir la liste complète des variables disponibles, consultez Variables d'environnement d'exécution définies.
- Initialiser la fonction – Charger le fichier de gestionnaire et exécuter tout code global ou statique qu'il contient. Les fonctions doivent créer des ressources statiques telles que des clients de kit SDK et des connexions de base de données une seule fois, puis les réutiliser pour plusieurs invocations.
- Gérer les erreurs : si une erreur se produit, appelez l'API erreur de l'initialisation et quittez immédiatement.

L'initialisation est comptabilisée dans le délai d'attente et la durée d'exécution facturés. Lorsqu'une exécution déclenche l'initialisation d'une nouvelle instance de votre fonction, vous pouvez voir le temps d'initialisation dans les journaux et le suivi AWS X-Ray.

Example journal

```
REPORT RequestId: f8ac1208... Init Duration: 48.26 ms   Duration: 237.17 ms   Billed
 Duration: 300 ms   Memory Size: 128 MB   Max Memory Used: 26 MB
```

Traitement des tâches

Pendant son exécution, l'environnement d'exécution utilise l'interface d'environnement d'exécution Lambda pour gérer les événements entrants et signaler des erreurs. Après avoir terminé les tâches d'initialisation, l'environnement d'exécution traite les événements entrants dans une boucle. Dans votre code d'exécution, effectuez les étapes suivantes dans l'ordre.

- Obtenir un événement – Appeler l'API d'invocation suivante pour obtenir l'événement suivant. Le corps de la réponse contient les données de l'événement. Les en-têtes de la réponse contiennent l'ID de la demande et d'autres informations.
- Propagation de l'en-tête de suivi : obtenez l'en-tête de X-Ray suivi à partir de l'`Lambda-Runtime-Trace-Id`en-tête de la réponse de l'API. Définissez la variable d'environnement `_X_AMZN_TRACE_ID` localement avec la même valeur. Le X-Ray SDK utilise cette valeur pour connecter les données de suivi entre les services.
- Créer un objet de contexte – Créer un objet avec des informations de contexte à partir des variables d'environnement et des en-têtes de la réponse de l'API.
- Invoquer le gestionnaire de fonctions – Transmettre l'événement et l'objet contexte au gestionnaire.
- Gérer la réponse – Appeler l'API réponse d'invocation pour afficher la réponse du gestionnaire.
- Gérer les erreurs : si une erreur se produit, appelez l'API erreur de l'invocation.
- Nettoyage : libérer les ressources inutilisées, envoyer des données à d'autres services ou accomplir des tâches supplémentaires avant de passer à l'événement suivant.

Entrypoint

Le point d'entrée d'un runtime personnalisé est un fichier exécutable nommé `bootstrap`. Le fichier d'amorçage peut être l'environnement d'exécution, ou il peut invoquer un autre fichier qui crée le runtime. Si la racine de votre package de déploiement ne contient pas de fichier nommé `bootstrap`, Lambda recherche le fichier dans les couches de la fonction. Si le fichier `bootstrap` n'existe pas ou

n'est pas exécutable, votre fonction renvoie une erreur `Runtime.InvalidEntrypoint` au moment de l'invocation.

Voici un exemple de `bootstrap` fichier qui utilise une version groupée de Node.js pour exécuter un JavaScript environnement d'exécution dans un fichier distinct nommé`runtime.js`.

Example bootstrap

```
#!/bin/sh
    cd $LAMBDA_TASK_ROOT
    ./node-v11.1.0-linux-x64/bin/node runtime.js
```

Implémentation du flux de réponses dans un environnement d'exécution personnalisé

Pour les fonctions de streaming de réponses, les points de terminaison `response` et `error` ont un comportement légèrement modifié qui permet à l'exécution de diffuser des réponses partielles au client et de renvoyer les charges utiles par morceaux. Pour plus d'informations sur le comportement spécifique, consultez ce qui suit :

- `/runtime/invocation/AwsRequestId/response` : propage l'en-tête `Content-Type` de l'environnement d'exécution pour l'envoyer au client. Lambda renvoie la charge utile de la réponse en morceaux en utilisant HTTP/1.1 un codage de transfert fragmenté. Pour envoyer le flux de réponse à Lambda, l'environnement d'exécution doit :
  - Définir l'en-tête HTTP `Lambda-Runtime-Function-Response-Mode` sur `streaming`.
  - Définissez l'en-tête `Transfer-Encoding` sur `chunked`.
  - Rédigez la réponse conformément à la spécification de codage de transfert HTTP/1.1 fragmenté.
  - Fermer la connexion sous-jacente après avoir écrit la réponse avec succès.
- `/runtime/invocation/AwsRequestId/error` : l'exécution peut utiliser ce point de terminaison pour signaler des erreurs de fonction ou d'exécution à Lambda, qui accepte également l'en-tête `Transfer-Encoding`. Ce point de terminaison ne peut être appelé qu'avant que l'environnement d'exécution ne commence à envoyer une réponse à l'invocation.
- Signaler les erreurs en cours de diffusion à l'aide des en-têtes de suivi d'erreur dans `/runtime/invocation/AwsRequestId/response`. Pour signaler les erreurs qui se produisent après que l'exécution commence à écrire la réponse à l'invocation, l'exécution peut optionnellement attacher des en-têtes de fin HTTP nommés `Lambda-Runtime-Function-Error-Type` et `Lambda-Runtime-Function-Error-Body`. Lambda considère cette réponse comme une réponse réussie et transmet les métadonnées d'erreur que l'exécution fournit au client.

> **Note**
>
> Pour joindre des en-têtes de fin, l'environnement d'exécution doit définir la valeur de l'en-tête `Trailer` au début de la demande HTTP. Il s'agit d'une exigence de la spécification de codage de transfert HTTP/1.1 fragmenté.

- `Lambda-Runtime-Function-Error-Type` : le type d'erreur que l'exécution a rencontré. Cet en-tête se compose d'une valeur de chaîne. Lambda accepte n'importe quelle chaîne, mais nous recommandons un format de. *`<category.reason>`* Par exemple : `Runtime.APIKeyNotFound`.
- `Lambda-Runtime-Function-Error-Body`— Base64-encoded des informations relatives à l'erreur.

Création d'environnements d'exécution personnalisés pour les instances gérées Lambda

Les instances gérées Lambda utilisent la même API d'exécution que les fonctions qui utilisent le fournisseur de capacité par défaut Lambda. Cependant, il existe des différences majeures dans la manière dont les environnements d'exécution personnalisés doivent être mis en œuvre pour prendre en charge le modèle d'exécution simultanée des instances gérées.

Gestion des demandes simultanées

La principale différence lors de la création d'environnements d'exécution personnalisés pour les instances gérées est la prise en charge des appels simultanés. Contrairement aux fonctions qui utilisent le fournisseur de capacité par défaut Lambda, où le moteur d'exécution traite un appel à la fois, les instances gérées peuvent traiter plusieurs appels simultanément au sein d'un même environnement d'exécution.

Votre environnement d'exécution personnalisé doit :

- Support des **`/next`** demandes simultanées : le moteur d'exécution peut effectuer plusieurs appels simultanés à l'API d'invocation suivante, dans la limite spécifiée par la variable d'`AWS_LAMBDA_MAX_CONCURRENCY`environnement.
- Gérer les **`/response`** demandes simultanées : plusieurs invocations peuvent appeler simultanément l'API de réponse à l'appel.

- Mettez en œuvre une gestion des demandes adaptée aux threads : assurez-vous que les appels simultanés n'interfèrent pas les uns avec les autres en gérant correctement les ressources et les états partagés.
- Utiliser correctement les identifiants de demande et d'invocation : un identifiant de demande identifie l'événement ; utilisez-le dans le chemin de l'URL. Un ID d'appel représente une seule tentative d'invocation : un seul ID de demande peut entraîner plusieurs tentatives, chacune avec un ID d'appel unique. Réactivez l'identifiant d'invocation `/response` et les `/error` appels. L'en-tête est facultatif ; son omission est acceptée pour des raisons de rétrocompatibilité. Lambda rejette uniquement with `400 InvalidInvocationId` lorsque l'en-tête est présent mais que sa valeur ne correspond pas.

Modèle de mise en œuvre

Un modèle d'implémentation typique pour les environnements d'exécution des instances gérées implique la création de threads de travail ou de processus pour gérer les invocations simultanées :

1. Lire la limite de simultanéité : lors de l'initialisation, lisez la variable d'`AWS_LAMBDA_MAX_CONCURRENCY`environnement pour déterminer le nombre d'appels simultanés à prendre en charge.
2. Créer un pool de travailleurs : initialisez un pool de travailleurs (threads, processus ou tâches asynchrones) égal à la limite de simultanéité.
3. Boucle de traitement des travailleurs — Chaque travailleur indépendamment :
   - Appels `/runtime/invocation/next` pour obtenir un événement d'invocation
   - Invoque le gestionnaire de fonctions avec les données de l'événement
   - Publie la réponse sur `/runtime/invocation/AwsRequestId/response`
   - Répète la boucle

Considérations supplémentaires

- Format de journalisation : les instances gérées ne prennent en charge que le format de journal JSON. Assurez-vous que votre environnement d'exécution respecte la variable d'`AWS_LAMBDA_LOG_FORMAT`environnement et utilise uniquement le format JSON. Pour plus d'informations, consultez Configuration des formats de journal JSON et en texte brut.

- Ressources partagées : soyez prudent lorsque vous utilisez des ressources partagées, telles que le `/tmp` répertoire avec des invocations simultanées. Mettez en place des mécanismes de verrouillage appropriés pour éviter les conditions de course.

Pour plus d'informations sur les environnements d'exécution des instances gérées Lambda, consultez. Comprendre l'environnement d'exécution des instances gérées Lambda

Tutoriel : création d’un environnement d’exécution personnalisé

Dans ce didacticiel, vous allez créer une fonction d'événement Lambda avec un environnement d'exécution personnalisé. Vous commencez par inclure le runtime dans le package de déploiement de la fonction. Ensuite, vous le migrez vers une couche que vous gérez indépendamment de la fonction. Enfin, vous partagez la couche du runtime en mettant à jour sa stratégie d’autorisations basée sur les ressources.

Conditions préalables

Ce didacticiel suppose que vous avez quelques connaissances des opérations Lambda de base et de la console Lambda. Si ce n’est déjà fait, suivez les instructions fournies dans Créer une fonction Lambda à l'aide de la console pour créer votre première fonction Lambda.

Pour effectuer les étapes suivantes, vous avez besoin de l’AWS CLI version 2. Les commandes et la sortie attendue sont répertoriées dans des blocs distincts :

```
aws --version
```

Vous devriez voir la sortie suivante:

```
aws-cli/2.13.27 Python/3.11.6 Linux/4.14.328-248.540.amzn2.x86_64 exe/x86_64.amzn.2
```

Pour les commandes longues, un caractère d’échappement (\) est utilisé pour les fractionner en plusieurs lignes.

Sur Linux et macOS, utilisez votre gestionnaire de shell et de package préféré.

> **Note**
>
> Sous Windows, certaines commandes CLI Bash que vous utilisez couramment avec Lambda (par exemple `zip`) ne sont pas prises en charge par les terminaux intégrés du système

d'exploitation. Pour obtenir une Windows-integrated version d'Ubuntu et de Bash, installez le sous-système Windows pour Linux. Les exemples de commandes CLI de ce guide utilisent le formatage Linux. Les commandes qui incluent des documents JSON en ligne doivent être reformatées si vous utilisez la CLI Windows.

Vous avez besoin d'un rôle IAM pour créer une fonction Lambda. Le rôle doit être autorisé à envoyer des CloudWatch journaux à Logs et à accéder aux Services AWS journaux utilisés par votre fonction. Si vous ne possédez pas de rôle pour le développement de fonction, créez-en un.

Pour créer un rôle d'exécution

1. Ouvrez la page Roles (Rôles) dans la console IAM.
2. Sélectionnez Créer un rôle.
3. Créez un rôle avec les propriétés suivantes :
   - Entité de confiance – Lambda.
   - Autorisations — AWSLambdaBasicExecutionRole.
   - Nom de rôle – **`lambda-role`**.

   La AWSLambdaBasicExecutionRolepolitique dispose des autorisations dont la fonction a besoin pour écrire des CloudWatch journaux dans Logs.

Créer une fonction

Créez une fonction d'événement Lambda avec un environnement d'exécution personnalisé. Cet exemple comprend deux fichiers : un fichier `bootstrap` d'exécution et un gestionnaire de fonctions. Tous deux sont mis en œuvre en Bash.

1. Créez un répertoire pour le projet, puis passez à ce répertoire.

   ```
   mkdir runtime-tutorial
   cd runtime-tutorial
   ```

2. Créez un nouveau fichier appelé `bootstrap`. Il s'agit de l'environnement d'exécution personnalisé.

Example bootstrap

```
#!/bin/sh

set -euo pipefail

# Initialization - load function handler
source $LAMBDA_TASK_ROOT/"$(echo $_HANDLER | cut -d. -f1).sh"

# Processing
while true
do
  HEADERS="$(mktemp)"
  # Get an event. The HTTP request will block until one is received
  EVENT_DATA=$(curl -sS -LD "$HEADERS" "http://
${AWS_LAMBDA_RUNTIME_API}/2018-06-01/runtime/invocation/next")

  # Extract request ID by scraping response headers received above
  REQUEST_ID=$(grep -Fi Lambda-Runtime-Aws-Request-Id "$HEADERS" | tr -d
 '[:space:]' | cut -d: -f2)

  # Extract invocation ID for cross-wiring protection
  INVOCATION_ID=$(grep -Fi Lambda-Runtime-Invocation-Id "$HEADERS" | tr -d
 '[:space:]' | cut -d: -f2)

  # Run the handler function from the script
  RESPONSE=$($(echo "$_HANDLER" | cut -d. -f2) "$EVENT_DATA")

  # Send the response, echoing the invocation ID
  curl "http://${AWS_LAMBDA_RUNTIME_API}/2018-06-01/runtime/invocation/$REQUEST_ID/
response"  -d "$RESPONSE" \
    ${INVOCATION_ID:+--header "Lambda-Runtime-Invocation-Id: $INVOCATION_ID"}
done
```

Le runtime charge un script de fonction à partir du package de déploiement. Il utilise deux variables pour localiser le script. `LAMBDA_TASK_ROOT` lui indique où le package a été extrait et `_HANDLER` inclut le nom du script.

Une fois que l'environnement d'exécution charge le script de la fonction, il utilise l'API d'exécution pour récupérer un événement d'invocation à partir de Lambda, transmet l'événement au gestionnaire, puis renvoie la réponse à Lambda. Pour obtenir l'ID de la demande, le runtime

enregistre les en-têtes à partir de la réponse de l'API dans un fichier temporaire et lit l'en-tête `Lambda-Runtime-Aws-Request-Id` à partir du fichier. Il lit également l'`Lambda-Runtime-Invocation-Id`en-tête et le renvoie dans la réponse.

> **Note**
>
> Les runtimes ont d'autres responsabilités, notamment la gestion des erreurs et la fourniture d'informations de contexte au gestionnaire. Pour plus d'informations, consultez Exigences.

3. Créez un script pour la fonction. L'exemple de script suivant définit une fonction de gestionnaire qui accepte les données des événements, la consigne dans `stderr`, puis la renvoie.

   Example function.sh

   ```
   function handler () {
     EVENT_DATA=$1
     echo "$EVENT_DATA" 1>&2;
     RESPONSE="Echoing request: '$EVENT_DATA'"

     echo $RESPONSE
   }
   ```

   Le répertoire `runtime-tutorial` devrait maintenant ressembler à ceci :

   ```
   runtime-tutorial
   # bootstrap
   # function.sh
   ```

4. Rendez les fichiers exécutables et ajoutez-les dans une archive ZIP. Vous obtiendrez alors le package de déploiement.

   ```
   chmod 755 function.sh bootstrap
   zip function.zip function.sh bootstrap
   ```

5. Créez une fonction nommée `bash-runtime`. Pour `--role`, entrez l'ARN de votre rôle d'exécution Lambda.

   ```
   aws lambda create-function --function-name bash-runtime \
   ```

```
--zip-file fileb://function.zip --handler function.handler --runtime
 provided.al2023 \
--role arn:aws:iam::123456789012:role/lambda-role
```

6. Invoquer la fonction.

```
aws lambda invoke --function-name bash-runtime --payload '{"text":"Hello"}'
 response.txt --cli-binary-format raw-in-base64-out
```

L'cli-binary-formatoption est obligatoire si vous utilisez AWS CLI la version 2. Pour faire de ce paramètre le paramètre par défaut, exécutez `aws configure set cli-binary-format raw-in-base64-out`. Pour plus d'informations, consultez les options de ligne de commande globales prises en charge par l'AWS CLI dans le Guide de l'utilisateur AWS Command Line Interface version 2.

Vous devriez obtenir une réponse comme celle-ci :

```
{
    "StatusCode": 200,
    "ExecutedVersion": "$LATEST"
}
```

7. Vérifiez la réponse.

```
cat response.txt
```

Vous devriez obtenir une réponse comme celle-ci :

```
Echoing request: '{"text":"Hello"}'
```

Créer une couche

Pour séparer le code du runtime du code de la fonction, créez une couche qui contient uniquement le runtime. Les couches vous permettent de développer les dépendances de votre fonction de manière indépendante et peuvent réduire l'utilisation du stockage lorsque vous utilisez la même couche avec plusieurs fonctions. Pour plus d'informations, consultez Gestion des dépendances des fonctions d'événement Lambda à l'aide de couches.

1. Créez un fichier .zip contient le fichier `bootstrap`.

```
zip runtime.zip bootstrap
```

2. Créez une couche avec la commande publish-layer-version.

```
aws lambda publish-layer-version --layer-name bash-runtime --zip-file fileb://
runtime.zip
```

Cela crée la première version de la couche.

Mettre à jour la fonction

Pour utiliser la couche d'exécution dans la fonction, configurez la fonction pour utiliser la couche et supprimez le code de l'environnement d'exécution de la fonction.

1. Mettez à jour la configuration de la fonction pour extraire la couche.

```
aws lambda update-function-configuration --function-name bash-runtime \
--layers arn:aws:lambda:us-east-1:123456789012:layer:bash-runtime:1
```

Cela ajoute le runtime à la fonction dans le répertoire `/opt`. Pour garantir que Lambda utilise l'environnement d'exécution dans la couche, vous devez supprimer `boostrap` du package de déploiement de la fonction, comme indiqué dans les deux étapes suivantes.

2. Créez un fichier .zip reprenant le code de la fonction.

```
zip function-only.zip function.sh
```

3. Mettez à jour le code de la fonction de façon à inclure uniquement le script du gestionnaire.

```
aws lambda update-function-code --function-name bash-runtime --zip-file fileb://
function-only.zip
```

4. Invoquez la fonction pour confirmer qu'elle fonctionne avec la couche de l'environnement d'exécution.

```
aws lambda invoke --function-name bash-runtime --payload '{"text":"Hello"}'
 response.txt --cli-binary-format raw-in-base64-out
```

L'cli-binary-formatoption est obligatoire si vous utilisez AWS CLI la version 2. Pour faire de ce paramètre le paramètre par défaut, exécutez `aws configure set cli-binary-format raw-in-base64-out`. Pour plus d'informations, consultez les options de ligne de commande globales prises en charge par l'AWS CLI dans le Guide de l'utilisateur AWS Command Line Interface version 2.

Vous devriez obtenir une réponse comme celle-ci :

```
{
    "StatusCode": 200,
    "ExecutedVersion": "$LATEST"
}
```

5. Vérifiez la réponse.

```
cat response.txt
```

Vous devriez obtenir une réponse comme celle-ci :

```
Echoing request: '{"text":"Hello"}'
```

Mettre à jour le runtime

1. Pour enregistrer des informations sur l'environnement d'exécution, mettez à jour le script du runtime pour générer les variables d'environnement.

Example bootstrap

```
#!/bin/sh

set -euo pipefail

# Configure runtime to output environment variables
echo "##  Environment variables:"
env

# Load function handler
source $LAMBDA_TASK_ROOT/"$(echo $_HANDLER | cut -d. -f1).sh"
```

```
# Processing
while true
do
  HEADERS="$(mktemp)"
  # Get an event. The HTTP request will block until one is received
  EVENT_DATA=$(curl -sS -LD "$HEADERS" "http://
${AWS_LAMBDA_RUNTIME_API}/2018-06-01/runtime/invocation/next")

  # Extract request ID by scraping response headers received above
  REQUEST_ID=$(grep -Fi Lambda-Runtime-Aws-Request-Id "$HEADERS" | tr -d
 '[:space:]' | cut -d: -f2)

  # Extract invocation ID for cross-wiring protection
  INVOCATION_ID=$(grep -Fi Lambda-Runtime-Invocation-Id "$HEADERS" | tr -d
 '[:space:]' | cut -d: -f2)

  # Run the handler function from the script
  RESPONSE=$($(echo "$_HANDLER" | cut -d. -f2) "$EVENT_DATA")

  # Send the response, echoing the invocation ID
  curl "http://${AWS_LAMBDA_RUNTIME_API}/2018-06-01/runtime/invocation/$REQUEST_ID/
response"  -d "$RESPONSE" \
    ${INVOCATION_ID:+--header "Lambda-Runtime-Invocation-Id: $INVOCATION_ID"}
done
```

2. Créez un fichier .zip reprenant la nouvelle version du fichier `bootstrap`.

```
zip runtime.zip bootstrap
```

3. Créer une nouvelle version de la couche `bash-runtime`.

```
aws lambda publish-layer-version --layer-name bash-runtime --zip-file fileb://
runtime.zip
```

4. Configurez la fonction pour utiliser la nouvelle version de la couche.

```
aws lambda update-function-configuration --function-name bash-runtime \
--layers arn:aws:lambda:us-east-1:123456789012:layer:bash-runtime:2
```

Partager la couche

Pour partager une couche avec une autre Compte AWS, ajoutez une déclaration d'autorisations entre comptes à la politique basée sur les ressources de la couche. Exécutez la commande add-layer-version-permission et spécifiez l'ID du compte en tant que `principal`. Dans chaque instruction, vous pouvez accorder une autorisation à un compte unique, à tous les comptes ou à une organisation dans AWS Organizations.

L'exemple suivant autorise le compte 111122223333 à accéder à la version 2 de la couche `bash-runtime`.

```
aws lambda add-layer-version-permission \
  --layer-name bash-runtime \
  --version-number 2 \
  --statement-id xaccount \
  --action lambda:GetLayerVersion \
  --principal 111122223333 \
  --output text
```

Vous devez voir des résultats similaires à ce qui suit :

```
{"Sid":"xaccount","Effect":"Allow","Principal":
{"AWS":"arn:aws:iam::111122223333:root"},"Action":"lambda:GetLayerVersion","Resource":"arn:aws:
east-1:123456789012:layer:bash-runtime:2"}
```

Les autorisations ne s'appliquent qu'à une seule version de couche. Répétez le processus chaque fois que vous créez une nouvelle version de la couche.

Nettoyage

Supprimez chaque version de la couche.

```
aws lambda delete-layer-version --layer-name bash-runtime --version-number 1
aws lambda delete-layer-version --layer-name bash-runtime --version-number 2
```

Étant donné que la fonction contient une référence à la version 2 de la couche, elle existe toujours dans Lambda. La fonction continue de fonctionner, mais les fonctions ne peuvent plus être configurées pour utiliser la version supprimée. Si vous modifiez la liste des couches sur la fonction, vous devez spécifier une nouvelle version ou omettre la couche supprimée.

Supprimez la fonction à l'aide de la commande delete-function.

```
aws lambda delete-function --function-name bash-runtime
```

Référentiels open source

AWS Lambda fournit une variété d'outils, de bibliothèques et de composants open source pour vous aider à créer, personnaliser et optimiser vos applications sans serveur. Ces ressources incluent des clients d'interface d'exécution, des bibliothèques d'événements, des images de base de conteneurs, des outils de développement et des exemples de projets gérés AWS et disponibles sur GitHub. En utilisant ces référentiels open source, vous pouvez étendre les fonctionnalités de Lambda, créer des environnements d'exécution personnalisés, traiter des événements provenant de différents AWS services et mieux comprendre les performances de votre fonction. Cette page fournit une présentation des principaux projets open source qui soutiennent le développement de Lambda.

Clients d’interface d’exécution

Les clients d’interface d’environnement d’exécution (RIC) Lambda sont des bibliothèques open source qui implémentent l’API d’exécution et gèrent l’interaction entre le code de votre fonction et le service Lambda. Ces clients gèrent la réception des événements d’invocation, la transmission des informations de contexte et le signalement des erreurs.

Les clients d’interface d’exécution utilisés par les environnements d’exécution gérés et les images de base de conteneurs de Lambda sont open source. Lorsque vous créez des environnements d’exécution personnalisés ou que vous étendez des environnements existants, vous pouvez utiliser ces bibliothèques open source pour simplifier la mise en œuvre. Les GitHub référentiels open source suivants contiennent le code source des RIC de Lambda :

- Node.js Client d'interface d'exécution
- Clients d’interface d’exécution Python
- Client d’interface d’environnement d’exécution Java
- Client d’interface d’environnement d’exécution Ruby
- Client d’interface d’exécution .NET
- Client d'interface d'exécution Rust
- Client d’interface d’environnement d’exécution Go
- Client d'interface Swift Runtime (expérimental)
- Client d'interface d'exécution C++ (expérimental)
- Images de base Lambda

Pour plus d'informations sur l'utilisation de ces clients pour créer une exécution personnalisée, consultez the section called "Création d'un environnement d'exécution personnalisé".

Bibliothèques d'événements

Les bibliothèques d'événements Lambda fournissent des définitions de type et des utilitaires d'assistance pour le traitement des événements provenant de différents services. AWS Ces bibliothèques vous aident à analyser et gérer les données d'événements de manière sécurisée, ce qui facilite l'utilisation d'événements provenant de services comme Amazon S3, Amazon DynamoDB et Amazon API Gateway.

Pour les langages compilés, AWS fournit les bibliothèques d'événements suivantes :

- Bibliothèque d'événements Java
- Bibliothèques d'événements .NET
- Bibliothèque d'événements Go
- Bibliothèque d'événements Rust

Pour les langages interprétés tels que Node.js Python et Ruby, les événements peuvent être analysés directement sous forme d'objets JSON sans nécessiter de bibliothèque séparée. Cependant, les développeurs qui utilisent Node.js Python peuvent utiliser PowerTools for AWS Lambda, qui fournit des schémas intégrés pour les AWS événements offrant des indications de type, une validation des données et des fonctionnalités similaires à celles fournies par les bibliothèques de langage compilées.

- Outils électriques pour TypeScript
- Powertools pour Python

Images de base de conteneur

AWS fournit des images de base de conteneurs open source que vous pouvez utiliser comme point de départ pour créer des images de conteneur pour vos fonctions d'événements Lambda. Ces images de base incluent le client d'interface d'environnement d'exécution et les autres composants nécessaires pour exécuter vos fonctions dans l'environnement d'exécution Lambda.

Pour plus d'informations sur les images de base disponibles et sur leur utilisation, consultez le référentiel Images de base AWS Lambda et the section called "Images de conteneurs".

Outils de développement

AWS fournit des outils de développement open source supplémentaires pour vous aider à créer et à optimiser vos fonctions Lambda :

Outils électriques pour AWS Lambda

Powertools for AWS Lambda simplifie le développement sans serveur grâce à des utilitaires essentiels pour empêcher le traitement en double, et au traitement par lots pour la gestion de plusieurs enregistrements et à la bibliothèque Kafka destinée aux consommateurs. Ces fonctionnalités vous aident à minimiser la complexité du code et les frais d'exploitation.

Vous pouvez également utiliser la validation intégrée du schéma d'événements, la journalisation et le suivi structurés, ainsi que l'intégration du magasin de paramètres, qui sont conçus pour accélérer la création de fonctions Lambda prêtes pour la production tout en suivant les AWS meilleures pratiques bien conçues.

GitHub référentiels :

- Python
- TypeScript
- Java
- .NET

Outils de développement Java

- Java Profiler (expérimental) : un outil pour profiler les fonctions Java Lambda.
- Bibliothèques Java : un référentiel qui contient une collection complète de bibliothèques et d'outils Java pour le développement Lambda, y compris des projets clés comme des utilitaires de test JUnit et des outils de profilage.
- Conteneur Java sans serveur : bibliothèque que vous pouvez utiliser pour exécuter des applications Java existantes sur Lambda avec un minimum de modifications.

Outils de développement .NET

Le référentiel AWS Lambda .NET fournit des bibliothèques et des outils .NET pour le développement Lambda, y compris des projets clés tels que les AWS Lambda outils pour la CLI .NET et le serveur .NET Core pour l'hébergement d'applications .NET Core.

Exemples de projets

Découvrez une collection complète d'exemples de projets et d'applications Lambda dans les référentiels Serverless Land. Ces exemples présentent différents cas d'utilisation, modèles d'intégration et bonnes pratiques Lambda pour vous aider à démarrer avec vos applications sans serveur.

Configuration AWS Lambda Fonctions événementielles

Découvrez comment configurer les fonctionnalités et options principales de votre fonction d'événement Lambda à l'aide de l'API ou de la console Lambda.

archives de fichiers .zip

Créez un package de déploiement de fonctions Lambda lorsque vous souhaitez inclure des dépendances, des couches d'exécution personnalisées ou des fichiers autres que le code de votre fonction. Le package de déploiement est une archive de fichier .zip contenant le code de votre fonction et ses dépendances.

Images de conteneur

Utilisez des images de conteneur pour empaqueter le code de votre fonction et ses dépendances lorsque vous avez besoin de mieux contrôler le processus de génération ou si votre fonction nécessite des configurations d'exécution personnalisées. Vous pouvez créer, tester et déployer des fonctions Lambda sous forme d'images de conteneur à l'aide d'outils tels que Docker CLI.

Self-managed Stockage de code S3

Configurez vos fonctions et vos couches pour utiliser votre propre compartiment S3 pour le stockage du code. Lambda référence votre code directement à partir de votre compartiment S3, éliminant ainsi les limites Lambda-managed de stockage et réduisant le délai de première invocation.

Mémoire

Découvrez comment et quand augmenter la mémoire des fonctions.

Stockage éphémère

Découvrez comment et quand augmenter la capacité de stockage temporaire de votre fonction.

Expiration

Découvrez comment et quand augmenter le délai d'expiration de votre fonction.

Variables d'environnement

Vous pouvez rendre le code de votre fonction portable et garder les secrets de votre code en les stockant dans la configuration de votre fonction à l'aide de variables d'environnement.

Réseaux sortants

Vous pouvez utiliser votre fonction Lambda avec les AWS ressources d'un Amazon VPC. La connexion de votre fonction à un VPC vous donne accès aux ressources d'un sous-réseau privé, telles que les bases de données relationnelles et les caches.

Réseaux entrants

Vous pouvez utiliser un point de terminaison d'un VPC d'interface pour invoquer vos fonctions Lambda sans traverser l'Internet public.

Système de fichiers

Vous pouvez utiliser votre fonction Lambda pour monter un Amazon EFS dans un répertoire local. Un système de fichiers permet à votre code de fonction d'accéder à des ressources partagées et de les modifier en toute sécurité et avec une simultanéité élevée.

Alias

Vous pouvez configurer vos clients pour qu'ils invoquent une version spécifique de la fonction Lambda en utilisant un alias, au lieu de mettre à jour le client.

Versions

En publiant une version de votre fonction, vous pouvez stocker votre code et votre configuration comme une ressource séparée qui ne peut pas être modifiée.

Balises

Utilisez des balises pour activer le contrôle d'accès basé sur les attributs (ABAC), pour organiser vos fonctions Lambda et pour filtrer et générer des rapports sur vos fonctions à l'aide des services ou AWS Billing and AWS Cost Explorer Cost Management.

Streaming des réponses

Vous pouvez configurer les URL de vos fonctions Lambda de manière à ce que les charges utiles des réponses soient renvoyées en continu aux clients. Le streaming de réponses peut profiter aux applications sensibles à la latence en améliorant les performances de temps au premier octet (TTFB). En effet, vous pouvez renvoyer des réponses partielles au client dès qu'elles sont

disponibles. En outre, vous pouvez utiliser le streaming de réponses pour créer des fonctions qui renvoient des charges utiles plus importantes.

Point final de métadonnées

Utilisez le point de terminaison de métadonnées Lambda pour découvrir dans quelle zone de disponibilité s'exécute votre fonction, ce qui vous permet d'optimiser la latence en acheminant vers des ressources de même zone de disponibilité et de mettre en œuvre des modèles de résilience. AZ-aware

Déploiement de fonctions événementielles Lambda sous forme d'archives de fichiers .zip

Lorsque vous créez une fonction d'événement Lambda, vous regroupez le code de votre fonction dans un package de déploiement. Lambda prend en charge deux types de packages de déploiement : les images conteneurs et les archives de fichier .zip. Le flux de travail de création d'une fonction dépend du type de package de déploiement. Pour configurer une fonction définie en tant qu'image de conteneur, consultez the section called “Images de conteneurs”.

Vous pouvez utiliser la console Lambda et l'API Lambda pour créer une fonction définie avec une archive de fichiers .zip. Vous pouvez également charger un fichier .zip mis à jour pour modifier le code de la fonction.

Par défaut, lorsque vous chargez un fichier .zip, Lambda stocke une copie de votre code source dans Lambda-managed rangement. Avec stockage de code S3 autogéré, Lambda lit votre code source depuis votre compartiment S3 lors des opérations de création et de mise à jour des fonctions, et ne stocke pas de copie séparée de votre code source. Lambda crée toujours une représentation interne optimisée de votre code pour l'invocation. Votre code source dans S3 n'est pas accessible à chaque démarrage à froid.

> **Note**
>
> Vous ne pouvez pas modifier le type de package de déploiement (.zip ou image de conteneur) d’une fonction existante. Par exemple, vous ne pouvez pas convertir une fonction d’image de conteneur pour utiliser un fichier d’archive .zip à la place. Vous devez créer une nouvelle fonction.

Rubriques

- Création de la fonction
- Utilisation de l'éditeur de code de la console
- Mise à jour du code de fonction
- Modification de l'environnement d'exécution
- Modification de l'architecture
- Utilisation de l'API Lambda
- Téléchargement du code de votre fonction

- CloudFormation
- Chiffrement des packages de déploiement Lambda au format .zip

Création de la fonction

Lorsque vous créez une fonction définie avec une archive de fichiers .zip, vous choisissez un modèle de code, la version du langage et le rôle d'exécution pour la fonction. Vous ajoutez votre code de fonction après que Lambda a créé la fonction.

Pour créer la fonction

1. Ouvrez le Page des fonctions de l'événement de la console Lambda.
2. Choisissez Créer une fonction d'événement.
3. Choisissez Créer à partir de zéro ou Utiliser un plan pour créer votre fonction.
4. Sous Informations de base, procédez comme suit :
    a. Pour Function name (Nom de la fonction), saisissez le nom de la fonction. Les noms de fonctions sont limités à 64 caractères.
    b. Pour Runtime, sélectionnez la version du langage à utiliser pour votre fonction.
    c. (Facultatif) Pour Architecture, choisissez l'architecture de l'ensemble des instructions pour utiliser la fonction. L'architecture par défaut est x86_64. Lorsque vous créez le package de déploiement de la fonction, assurez-vous qu'il est compatible avec cette architecture de l'ensemble des instructions.
5. (Facultatif) Sous Permissions (Autorisations), développez Change default execution role (Modifier le rôle d'exécution par défaut). Vous pouvez créer un rôle d'exécution ou utiliser un rôle existant.
6. (Facultatif) Développez Advanced settings (Paramètres avancés). Vous pouvez choisir une Configuration de signature de code pour la fonction. Vous pouvez également configurer un (VPC Amazon) auquel la fonction puisse accéder.
7. Choisissez Créer une fonction d'événement.

Lambda crée la nouvelle fonction. Vous pouvez désormais utiliser la console pour ajouter le code de fonction et configurer d'autres paramètres et caractéristiques de la fonction. Pour obtenir des instructions de déploiement de code, consultez la page du gestionnaire pour l'exécution utilisée par votre fonction.

Node.js

- Déployez les fonctions d'événement Node.js Lambda avec des archives de fichiers .zip

Python

- Utilisation d'archives de fichiers .zip pour les fonctions événementielles Lambda en Python

Ruby

- Déployez les fonctions d'événement Ruby Lambda avec des archives de fichiers .zip

Java

- Déployez les fonctions d'événement Java Lambda avec des archives de fichiers .zip ou JAR

Go

- Déployez les fonctions d'événement Go Lambda avec des archives de fichiers .zip

C#

- Créez et déployez des fonctions d'événement Lambda C# avec des archives de fichiers .zip

PowerShell

- Déployez les fonctions d'événement PowerShell Lambda avec des archives de fichiers .zip

Utilisation de l'éditeur de code de la console

La console crée une fonction Lambda avec un seul fichier source. Pour le scripting, vous pouvez modifier ce fichier et ajouter des fichiers à l'aide de l'éditeur de code intégré. Choisissez Save pour enregistrer les changements. Ensuite, pour exécuter votre code, choisissez Test.

Lorsque vous enregistrez votre code de fonction, la console Lambda crée un package de déploiement d'archive de fichiers .zip. Lorsque vous développez votre code de fonction en dehors de la console (à l'aide d'un IDE), vous devez créer un package de déploiement pour charger votre code dans la fonction Lambda.

Mise à jour du code de fonction

Pour les langages de script (Node.js, Python et Ruby), vous pouvez modifier le code de votre fonction dans l'éditeur de code intégré. Si ce code est d'une taille supérieure à 3 Mo, si vous devez ajouter des bibliothèques ou dans le cas des langages que l'éditeur ne prend pas en charge (Java, Go, C#), vous devez charger le code de votre fonction en tant qu'archive .zip. Si l'archive de fichier .zip est d'une taille inférieure à 50 Mo, vous pouvez charger l'archive de fichier .zip à partir de votre machine

locale. Si le fichier est d'une taille supérieure à 50 Mo, chargez le fichier dans la fonction à partir d'un compartiment Amazon S3.

Pour charger le code de fonction en tant qu'archive .zip

1. Ouvrez le Page des fonctions de l'événement de la console Lambda.
2. Sélectionnez la fonction à mettre à jour, puis choisissez l'onglet Code.
3. Sous Code source (Source du code), sélectionnez Upload from (Charger depuis).
4. Choisissez .zip file (fichier .zip), puis Upload (Charger).
    - Dans le sélecteur de fichiers, sélectionnez la nouvelle version de l'image et choisissez Open (Ouvrir), puis Save (Enregistrer).
5. (Alternative à l'étape 4) Choisissez Emplacement Amazon S3.
    a. Dans la zone de texte, entrez l'URL du lien S3 de l'archive du fichier .zip.
    b. En dessous Mode de stockage de code, choisissez l'une des options suivantes :
        - Mode copie (par défaut)
        - Mode de référence
    c. Cliquez sur Enregistrer.

Lors de la mise à jour du code de fonction depuis un compartiment Amazon S3 à l'aide du AWS CLI, vous pouvez spécifier le mode de stockage du code. Set `S3ObjectStorageMode` pour `REFERENCE` à utiliser stockage de code S3 autogéré, ou `COPY` (par défaut) à utiliser Lambda-managed rangement. Vous pouvez modifier le mode de stockage à chaque mise à jour.

```
aws lambda update-function-code \
  --function-name my-function \
  --s3-bucket my-bucket \
  --s3-key my-function.zip \
  --s3-object-version abc123 \
  --s3-object-storage-mode REFERENCE
```

Modification de l'environnement d'exécution

Si vous mettez à jour la configuration de la fonction pour utiliser un nouveau moteur d'exécution, vous devrez peut-être mettre à jour le code de la fonction pour qu'il soit compatible avec le nouveau moteur d'exécution. Si vous mettez à jour la configuration de la fonction pour utiliser une

autre exécution, vous devez fournir un nouveau code de fonction compatible avec l'exécution et l'architecture. Pour obtenir des instructions sur comment créer un package de déploiement pour le code de la fonction, consultez la page du gestionnaire de l'exécution utilisé par la fonction.

Le Node.js Les images de base 20, Python 3.12, Java 21, .NET 8, Ruby 3.3 et versions ultérieures sont basées sur l'image de conteneur minimale Amazon Linux 2023. Les images de base antérieures utilisaient Amazon Linux 2. AL2023 offre plusieurs avantages par rapport à Amazon Linux2, notamment un encombrement de déploiement réduit et des versions mises à jour de bibliothèques telles que `glibc`. Pour plus d'informations, consultez Présentation de l'environnement d'exécution Amazon Linux 2023 pour AWS Lambda sur le blog AWS Compute.

Pour modifier l'environnement d'exécution

1. Ouvrez le Page des fonctions de l'événement de la console Lambda.
2. Sélectionnez la fonction à mettre à jour, puis choisissez l'onglet Code.
3. Faites défiler jusqu'à la section Runtime settings (Paramètres d'exécution), qui se trouve sous l'éditeur de code.
4. Choisissez Modifier.
    a. Pour Runtime (Environnement d'exécution), sélectionnez l'identifiant de l'environnement d'exécution.
    b. Pour Gestionnaire, spécifiez le nom de fichier et gestionnaire de votre fonction.
    c. Pour Architecture, choisissez l'architecture de l'ensemble des instructions pour utiliser votre fonction.
5. Cliquez sur Enregistrer.

Modification de l'architecture

Avant de pouvoir modifier l'architecture de l'ensemble des instructions, vous devez vous assurer que le code de la fonction est compatible avec l'architecture cible.

Si vous utilisez Node.js, Python ou Ruby et si vous modifiez le code de votre fonction dans l'éditeur intégré, le code existant peut s'exécuter sans modification.

Toutefois, si vous fournissez le code de fonction en utilisant un package de déploiement d'archives de fichiers .zip, vous devez préparer une nouvelle archive de fichiers .zip compilée et créée correctement pour l'exécution cible et l'architecture de l'ensemble des instructions. Pour obtenir des instructions, veuillez consulter la page du gestionnaire d'exécution de la fonction.

Pour modifier l'architecture de l'ensemble des instructions

1. Ouvrez le Page des fonctions de l'événement de la console Lambda.
2. Sélectionnez la fonction à mettre à jour, puis choisissez l'onglet Code.
3. Sous Paramètres du runtime, choisissez Modifier.
4. Pour Architecture, choisissez l'architecture de l'ensemble des instructions pour utiliser votre fonction.
5. Cliquez sur Enregistrer.

Utilisation de l'API Lambda

Pour créer et configurer une fonction qui utilise une archive de fichiers .zip, utilisez les opérations d'API suivantes :

- CreateFunction
- UpdateFunctionCode
- UpdateFunctionConfiguration

Téléchargement du code de votre fonction

Vous pouvez télécharger la version inédite actuelle (`$LATEST`) version de votre code de fonction .zip depuis la console Lambda. Avant de démarrer, vérifiez que vous disposez des autorisations IAM suivantes :

- `iam:GetPolicy`
- `iam:GetPolicyVersion`
- `iam:GetRole`
- `iam:GetRolePolicy`
- `iam:ListAttachedRolePolicies`
- `iam:ListRolePolicies`
- `iam:ListRoles`

Pour télécharger l’archive .zip du code de fonction

1. Ouvrez le Page des fonctions de l'événement de la console Lambda.

2. Sélectionnez la fonction pour laquelle vous souhaitez télécharger l'archive .zip du code de la fonction.
3. Dans Aperçu de la fonction, cliquez sur le bouton Télécharger, puis choisissez Télécharger l'archive .zip du code de fonction

    - Vous pouvez également choisir Télécharger AWS SAM fichier pour générer et télécharger un modèle SAM basé sur la configuration de votre fonction. Vous pouvez aussi choisir Télécharger les deux pour télécharger à la fois l'archive .zip et le modèle SAM.

CloudFormation

Vous pouvez utiliser CloudFormation pour créer une fonction Lambda qui utilise une archive de fichiers .zip. Dans votre CloudFormation modèle, le `AWS::Lambda::Function` resource spécifie la fonction Lambda. Pour les descriptions des propriétés dans le `AWS::Lambda::Function` ressource, voir AWS::Lambda::Fonction dans le AWS CloudFormation Guide de l'utilisateur.

Dans la ressource `AWS::Lambda::Function`, définissez les propriétés suivantes pour créer une fonction définie en tant qu'archive de fichiers .zip :

- AWS::Lambda::Fonction
    - PackageType — Réglez sur `Zip`.
    - Code – Saisissez le nom du compartiment Amazon S3 et le nom du fichier .zip dans les champs `S3Bucket` et `S3Key`. Pour Node.js ou Python, vous pouvez fournir le code source en ligne de votre fonction Lambda.
    - Runtime – Définissez la valeur du runtime.
    - Architecture : définissez la valeur de l'architecture sur `arm64` à utiliser AWS Processeurs Graviton. La valeur de l'architecture par défaut est `x86_64`.
    - S3ObjectStorageMode — (Facultatif) Réglez sur `REFERENCE` à utiliser stockage de code S3 autogéré. Réglez sur `COPY` (par défaut) à utiliser Lambda-managed rangement.

Chiffrement des packages de déploiement Lambda au format .zip

AWS Lambda fournit toujours un chiffrement côté serveur au repos pour les packages de déploiement .zip et les détails de configuration des fonctions avec un. AWS KMS key Par défaut, Lambda utilise une Clé détenue par AWS. Si ce comportement par défaut convient à votre flux de travail, vous n'avez rien d'autre à configurer. AWS l'utilisation de cette clé ne vous est pas facturée.

Si vous préférez, vous pouvez plutôt fournir une clé gérée par le AWS KMS client. Vous pouvez procéder ainsi pour contrôler la rotation de la clé KMS ou pour répondre aux exigences de votre organisation en matière de gestion des clés KMS. Lorsque vous utilisez une clé gérée par le client, seuls les utilisateurs de votre compte ayant accès à la clé KMS peuvent visualiser ou gérer le code ou la configuration de la fonction.

Les clés gérées par le client entraînent des AWS KMS frais standard. Pour en savoir plus, consultez Pricing AWS Key Management Service (Tarification).

Création d'une clé gérée par le client

Vous pouvez créer une clé symétrique gérée par le client à l'aide de Console de gestion AWS, ou des AWS KMS API.

Pour créer une clé symétrique gérée par le client

Suivez les étapes de la rubrique Create a symmetric encryption KMS key dans le Guide du développeur AWS Key Management Service .

Permissions

Stratégie de clé

Les stratégies de clé contrôlent l'accès à votre clé gérée par le client. Chaque clé gérée par le client doit avoir exactement une stratégie de clé, qui contient des instructions qui déterminent les personnes pouvant utiliser la clé et comment elles peuvent l'utiliser. Pour plus d'informations, consultez How to change a key policy dans le Guide du développeur AWS Key Management Service .

Lorsque vous utilisez une clé gérée par le client pour chiffrer un package de déploiement .zip, Lambda n'ajoute aucun octroi à la clé. Au lieu de cela, votre politique AWS KMS clé doit autoriser Lambda à appeler les opérations d' AWS KMS API suivantes en votre nom :

- km : GenerateDataKey
- kms:Decrypt

L'exemple de politique de clé suivant permet à toutes les fonctions Lambda du compte 111122223333 d'appeler les AWS KMS opérations requises pour la clé gérée par le client spécifiée :

Example AWS KMS politique clé

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "lambda.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Resource": "arn:aws:kms:us-east-1:111122223333:key/key-id",
            "Condition": {
                "StringLike": {
                "kms:EncryptionContext:aws:lambda:FunctionArn":
 "arn:aws:lambda:us-east-1:111122223333:function:*"
                }
            }
        }
    ]
}
```

Pour plus d'informations sur le dépannage des clés d'accès, consultez le Guide du développeur AWS Key Management Service .

Autorisations de principal

Lorsque vous utilisez une clé gérée par le client pour chiffrer un package de déploiement .zip, seuls les principaux ayant accès à cette clé peuvent accéder au package de déploiement .zip. Par exemple, les principaux qui n'ont pas accès à la clé gérée par le client ne peuvent pas télécharger le package .zip à l'aide de l'URL S3 présignée incluse dans la réponse. GetFunction Une `AccessDeniedException` est renvoyée dans la section `Code` de la réponse.

Example AWS KMS AccessDeniedException

```
{
```

```
    "Code": {
        "RepositoryType": "S3",
        "Error": {
            "ErrorCode": "AccessDeniedException",
            "Message": "KMS access is denied. Check your KMS permissions. KMS
 Exception: AccessDeniedException KMS Message: User: arn:aws:sts::111122223333:assumed-
role/LambdaTestRole/session is not authorized to perform: kms:Decrypt on resource:
 arn:aws:kms:us-east-1:111122223333:key/key-id with an explicit deny in a resource-
based policy"
        },
        "SourceKMSKeyArn": "arn:aws:kms:us-east-1:111122223333:key/key-id"
    },
 ...
```

Pour plus d'informations sur les autorisations relatives aux AWS KMS clés, consultez Authentification et contrôle d'accès pour AWS KMS.

Utilisation d’une clé gérée par le client pour votre package de déploiement .zip

Utilisez les paramètres d’API suivants pour configurer les clés gérées par le client pour les packages de déploiement .zip :

- SourceKMSKeyArn: chiffre le package de déploiement .zip source (le fichier que vous chargez).
- KMSKeyArn: chiffre les variables d'environnement et les instantanés SnapStart Lambda.
- DurableConfig.KMSKeyArn: chiffre les données d'exécution durables. Cette touche est indépendante du niveau de fonction. `KMSKeyArn`

Lorsque `SourceKMSKeyArn` et `KMSKeyArn` sont tous deux spécifiés, Lambda utilise la clé `KMSKeyArn` pour chiffrer la version décompressée du package que Lambda utilise pour invoquer la fonction. Lorsque `SourceKMSKeyArn` est spécifié mais que `KMSKeyArn` ne l’est pas, Lambda utilise une Clé gérée par AWSpour chiffrer la version décompressée du package.

> **Note**
>
> Pour les fonctions et les couches qui utilisent le stockage de code S3 autogéré, Lambda ne stocke aucune copie de votre code source. Votre code reste dans votre compartiment S3, et le chiffrement au repos de votre code source est géré par la configuration de votre compartiment S3. Lambda utilisera `KMSKeyArn` pour chiffrer la version décompressée du package que Lambda utilise pour appeler la fonction. Pour plus d'informations, consultez la

section Protection des données avec le chiffrement côté serveur dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Lambda console

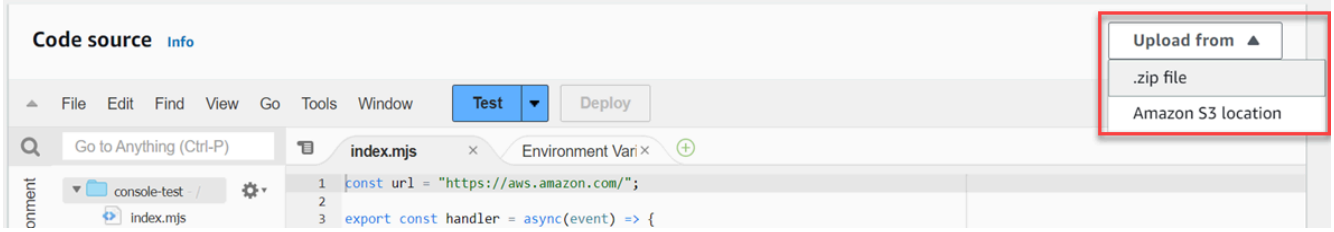
Pour ajouter un chiffrement par clé gérée par le client lors de la création d'une fonction

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez Create Event Function.
3. Choisissez Author from scratch (Créer à partir de zéro) ou Container image (Image de conteneur).
4. Sous Basic information (Informations de base), procédez comme suit :
   a. Pour Function name (Nom de la fonction), saisissez le nom de la fonction.
   b. Pour Runtime, sélectionnez la version du langage à utiliser pour votre fonction.
5. Développez les paramètres avancés, puis sélectionnez Activer le chiffrement avec une clé gérée par AWS KMS le client.
6. Choisissez une clé gérée par le client.
7. Choisissez Create Event Function.

Pour supprimer le chiffrement par clé gérée par le client ou pour utiliser une autre clé, vous devez télécharger à nouveau le package de déploiement .zip.

Pour ajouter le chiffrement par clé gérée par le client à une fonction existante

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez le nom d'une fonction.
3. Dans le volet Source du code, choisissez Charger à partir de.
4. Choisissez un fichier .zip ou un emplacement Amazon S3.



5. Importez le fichier ou saisissez l'emplacement Amazon S3.
6. Choisissez Activer le chiffrement avec une clé gérée par le AWS KMS client.
7. Choisissez une clé gérée par le client.
8. Cliquez sur Enregistrer.

AWS CLI

Pour ajouter un chiffrement par clé gérée par le client lors de la création d'une fonction

Dans l'exemple create-function suivant :

- `--code`: Spécifie le chemin local vers le package de déploiement .zip (`ZipFile`) et la clé gérée par le client pour le chiffrer ()`SourceKMSKeyArn`.
- `--kms-key-arn` : spécifie la clé gérée par le client pour chiffrer les variables d'environnement et la version décompressée du package de déploiement.

```
aws lambda create-function \
  --function-name myFunction \
  --runtime nodejs24.x \
  --handler index.handler \
  --role arn:aws:iam::111122223333:role/service-role/my-lambda-role \
  --code ZipFile=fileb://myFunction.zip,SourceKMSKeyArn=arn:aws:kms:us-
east-1:111122223333:key/key-id \
  --kms-key-arn arn:aws:kms:us-east-1:111122223333:key/key2-id
```

Dans l'exemple create-function suivant :

- `--code`: Spécifie l'emplacement du fichier .zip dans un compartiment Amazon S3 (`S3Bucket`,`S3Key`,`S3ObjectVersion`) et la clé gérée par le client pour le chiffrer (`SourceKMSKeyArn`).
- `--kms-key-arn` : spécifie la clé gérée par le client pour chiffrer les variables d'environnement et la version décompressée du package de déploiement.

```
aws lambda create-function \
  --function-name myFunction \
  --runtime nodejs24.x --handler index.handler \
  --role arn:aws:iam::111122223333:role/service-role/my-lambda-role \
```

```
  --code S3Bucket=amzn-s3-demo-
bucket,S3Key=myFileName.zip,S3ObjectVersion=myObjectVersion,SourceKMSKeyArn=arn:aws:kms:us-
east-1:111122223333:key/key-id \
  --kms-key-arn arn:aws:kms:us-east-1:111122223333:key/key2-id
```

Pour ajouter un chiffrement par clé gérée par le client à une fonction existante

Dans l'exemple update-function-code suivant :

- `--zip-file` : spécifie le chemin local du package de déploiement .zip.
- `--source-kms-key-arn` : spécifie la clé gérée par le client pour chiffrer la version compressée du package de déploiement. Lambda utilise une clé AWS détenue pour chiffrer le package décompressé pour les invocations de fonctions. Si vous souhaitez utiliser une clé gérée par le client pour chiffrer la version décompressée du package, exécutez la commande update-function-configuration avec l'option `--kms-key-arn`.

```
aws lambda update-function-code \
  --function-name myFunction \
  --zip-file fileb://myFunction.zip \
  --source-kms-key-arn arn:aws:kms:us-east-1:111122223333:key/key-id
```

Dans l'exemple update-function-code suivant :

- `--s3-bucket` : spécifie l'emplacement du fichier .zip dans un compartiment Amazon S3.
- `--s3-key` : spécifie la clé Amazon S3 du package de déploiement.
- `--s3-object-version` : pour les objets versionnés, la version de l'objet de package de déploiement à utiliser.
- `--source-kms-key-arn` : spécifie la clé gérée par le client pour chiffrer la version compressée du package de déploiement. Lambda utilise une clé AWS détenue pour chiffrer le package décompressé pour les invocations de fonctions. Si vous souhaitez utiliser une clé gérée par le client pour chiffrer la version décompressée du package, exécutez la commande update-function-configuration avec l'option `--kms-key-arn`.

```
aws lambda update-function-code \
  --function-name myFunction \
  --s3-bucket amzn-s3-demo-bucket \
  --s3-key myFileName.zip \
```

```
  --s3-object-version myObject Version
  --source-kms-key-arn arn:aws:kms:us-east-1:111122223333:key/key-id
```

Pour supprimer le chiffrement par clé gérée par le client d'une fonction existante

Dans l'exemple update-function-code suivant, `--zip-file` spécifie le chemin local vers le package de déploiement .zip. Lorsque vous exécutez cette commande sans `--source-kms-key-arn` option, Lambda utilise une clé AWS détenue pour chiffrer la version compressée du package de déploiement.

```
aws lambda update-function-code \
  --function-name myFunction \
  --zip-file fileb://myFunction.zip
```

Création d'une fonction d'événement Lambda à l'aide d'une image de conteneur

Le code de votre AWS Lambda fonction se compose de scripts ou de programmes compilés et de leurs dépendances. Pour déployer votre code de fonction vers Lambda, vous utilisez un package de déploiement. Lambda prend en charge deux types de packages de déploiement : les images conteneurs et les archives de fichiers .zip.

Il existe trois méthodes pour créer une image de conteneur pour une fonction Lambda :

- À l'aide d'un AWS image de base pour Lambda

  Les images de base AWS sont préchargées avec une exécution du langage, un client d'interface d'exécution pour gérer l'interaction entre Lambda et votre code de fonction, et un émulateur d'interface d'exécution pour les tests locaux.
- À l'aide d'un AWS OS-only image de base

  AWS OS-only les images de base contiennent une distribution Amazon Linux et l'émulateur d'interface d'exécution. Ces images sont couramment utilisées pour créer des images de conteneur pour les langages compilés, tels que Go et Rust, et pour une langue ou une version linguistique pour laquelle Lambda ne fournit pas d'image de base, telle que Node.js 19. Vous pouvez également utiliser des images OS-only de base pour implémenter un environnement d'exécution personnalisé. Pour rendre l'image compatible avec Lambda, vous devez inclure un client d'interface d'exécution pour votre langage dans l'image.
- En utilisant un non-AWS image de base

  Vous pouvez utiliser une autre image de base à partir d'un autre registre de conteneur, comme Alpine Linux ou Debian. Vous pouvez également utiliser une image personnalisée créée par votre organisation. Pour rendre l'image compatible avec Lambda, vous devez inclure un client d'interface d'exécution pour votre langage dans l'image.

> **Tip**
>
> Pour réduire le temps nécessaire à l'activation des fonctions du conteneur Lambda, consultez Utiliser des générations en plusieurs étapes (français non garanti) dans la documentation Docker. Pour créer des images de conteneur efficaces, suivez la section Bonnes pratiques pour l'écriture de Dockerfiles (français non garanti).

Pour créer une fonction Lambda à partir d'une image de conteneur, créez votre image localement et chargez-la dans un référentiel Amazon Elastic Container Registry (Amazon ECR). Si vous utilisez une image de conteneur fournie par un vendeur AWS Marketplace, vous devez d'abord cloner l'image dans votre référentiel Amazon ECR privé. Indiquez ensuite l'URI du référentiel lorsque vous créez la fonction. Le référentiel Amazon ECR doit être Région AWS identique à la fonction Lambda. Vous pouvez créer une fonction en utilisant une image d'un autre AWS compte, à condition que l'image se trouve dans la même région que la fonction Lambda. Pour plus d'informations, consultez Autorisations entre comptes Amazon ECR.

> **Note**
>
> Lambda ne prend pas en charge les points de terminaison Amazon ECR FIPS pour les images de conteneurs. Si l'URI de votre dépôt contient `ecr-fips`, vous utilisez un point de terminaison FIPS. Exemple: `111122223333.dkr.ecr-fips.us-east-1.amazonaws.com`.

Cette page explique les types d'images de base et les exigences relatives à la création d'images de Lambda-compatible conteneur.

> **Note**
>
> Vous ne pouvez pas modifier le type de package de déploiement (.zip ou image de conteneur) d'une fonction existante. Par exemple, vous ne pouvez pas convertir une fonction d'image de conteneur pour utiliser un fichier d'archive .zip à la place. Vous devez créer une nouvelle fonction.

Rubriques

- Exigences
- À l'aide d'un AWS image de base pour Lambda
- À l'aide d'un AWS OS-only image de base
- En utilisant un non-AWS image de base
- Clients d'interface d'exécution
- Autorisations Amazon ECR
- Cycle de vie des fonctions

Exigences

Installez l'AWS CLI version 2 et la CLI Docker. En outre, notez les exigences suivantes :

- L'image de conteneur doit implémenter l'Utilisation de l'API de l'environnement d'exécution Lambda pour des environnements d'exécution personnalisés. Les clients d'interface de runtime open source AWS implémentent l'API. Vous pouvez ajouter un client d'interface de runtime à votre image de base préférée pour la rendre compatible avec Lambda.
- L'image de conteneur doit pouvoir s'exécuter sur un système de fichiers en lecture seule. Votre code de fonction peut accéder à un répertoire `/tmp` inscriptible entre 512 Mo et 10 240 Mo de stockage, par incréments de 1 Mo.
- L'utilisateur Lambda par défaut doit pouvoir lire tous les fichiers requis pour exécuter votre code de fonction. Lambda suit les bonnes pratiques de sécurité en définissant un utilisateur Linux par défaut avec des autorisations assortie d'un privilège minimum. Cela signifie que vous n'avez pas besoin de spécifier un UTILISATEUR dans votre Dockerfile. Vérifiez que votre code d'application ne repose pas sur des fichiers dont l'exécution n'est pas autorisée à d'autres utilisateurs Linux.
- Lambda ne prend en charge que les images de Linux-based conteneurs.
- Lambda fournit des images de base multi-architecture. Toutefois, l'image que vous créez pour la fonction ne doit avoir que l'une des architectures pour cible. Lambda ne prend pas en charge les fonctions qui utilisent les images de conteneur multi-architecture.

À l'aide d'un AWS image de base pour Lambda

Vous pouvez utiliser l'une des images de base AWS pour Lambda afin de créer l'image de conteneur pour votre code de fonction. Les images de base sont préchargées avec une exécution de langage et d'autres composants requis pour exécuter une image conteneur sur Lambda. Vous ajoutez votre code de fonction et vos dépendances à l'image de base, puis vous l'empaquetez en tant qu'image de conteneur.

AWS fournit régulièrement des mises à jour des images AWS de base pour Lambda. Si votre Dockerfile inclut le nom de l'image dans la propriété FROM, votre client Docker extrait la dernière version de l'image du référentiel Amazon ECR. Afin d'utiliser l'image de base mise à jour, vous devez reconstruire votre image de conteneur et mettre à jour le code de la fonction.

Les images de base Node.js 20, Python 3.12, Java 21, .NET 8, Ruby 3.3 et versions ultérieures sont basées sur l'image de conteneur minimale Amazon Linux 2023. Les images de base antérieures utilisaient Amazon Linux 2. AL2023 offre plusieurs avantages par rapport à Amazon Linux2,

notamment un encombrement de déploiement réduit et des versions mises à jour de bibliothèques telles que `glibc`.

AL2023-based les images utilisent `microdnf` (lié par un lien symboliquednf) comme gestionnaire de packages au lieu deyum, qui est le gestionnaire de packages par défaut dans Amazon Linux 2. `microdnf`est une implémentation autonome de. `dnf` Pour obtenir la liste des packages inclus dans les AL2023-based images, reportez-vous aux colonnes Conteneur minimal de la section Comparaison des packages installés sur Amazon Linux 2023 Container Images. Pour plus d'informations sur les différences entre AL2023 et Amazon Linux 2, consultez Introducing the Amazon Linux 2023 runtime for AWS Lambda sur le blog AWS Compute.

> **Note**
>
> Pour exécuter AL2023-based des images localement, y compris avec AWS Serverless Application Model (AWS SAM), vous devez utiliser Docker version 20.10.10 ou ultérieure.

Pour créer une image de conteneur à l'aide d'une image de AWS base, choisissez les instructions correspondant à votre langue préférée :

- Node.js
- TypeScript(utilise une image Node.js de base)
- Python
- Java
- Go
- .NET
- Ruby

À l'aide d'un AWS OS-only image de base

AWS OS-only les images de base contiennent une distribution Amazon Linux et l'émulateur d'interface d'exécution. Ces images sont couramment utilisées pour créer des images de conteneur pour les langages compilés, tels que Go et Rust, et pour une langue ou une version linguistique pour laquelle Lambda ne fournit pas d'image de base, telle que Node.js 19. Vous pouvez également utiliser des images OS-only de base pour implémenter un environnement d'exécution personnalisé. Pour rendre l'image compatible avec Lambda, vous devez inclure un client d'interface d'exécution pour votre langage dans l'image.

Étiquett s	Environne ment d'exécution	Système d'exploit ation	Dockerfile	Obsolescence
al2023	OS-only Durée d'exécution	Amazon Linux	Dockerfile pour OS-only Runtime sur GitHub	30 juin 2029

Galerie publique d'Amazon Elastic Container Registry : gallery.ecr. aws/lambda/fourni

En utilisant un non-AWS image de base

Lambda prend en charge toute image conforme à l'un des formats de manifeste d'image suivants :

- Manifeste d'images Docker V2, schéma 2 (utilisé avec la version 1.10 de Docker et les versions les plus récentes)
- Spécifications OCI (Open Container initiative, soit initiative de conteneur ouvert) (v1.0.0 et versions ultérieures)

Lambda prend en charge une taille maximale d'image non compressée de 10 Go, comprenant toutes les couches.

> **Note**
>
> - Pour rendre l'image compatible avec Lambda, vous devez inclure un client d'interface d'exécution pour votre langage dans l'image.
> - Pour des performances optimales, maintenez la taille de votre manifeste d'image inférieure à 25 400 octets. Pour réduire la taille du manifeste d'image, réduisez le nombre de couches de votre image et réduisez le nombre d'annotations.

Clients d'interface d'exécution

Si vous utilisez une image OS-only de base ou une image de base alternative, vous devez inclure un client d'interface d'exécution dans votre image. Le client de l'interface d'exécution doit étendre leUtilisation de l'API de l'environnement d'exécution Lambda pour des environnements d'exécution

personnalisés, qui gère l'interaction entre Lambda et votre code de fonction. AWS fournit des clients d'interface d'exécution open source pour les langages suivants :

- Node.js
- Python
- Java
- .NET
- Go
- Ruby
- Rouille —

Si vous utilisez un langage qui ne possède pas de client d'interface d'exécution AWS fourni, vous devez créer le vôtre.

Autorisations Amazon ECR

Avant de créer une fonction Lambda à partir d'une image de conteneur, vous devez créer l'image localement et la charger dans un référentiel Amazon ECR. Lorsque vous créez la fonction, indiquez l'URI du référentiel Amazon ECR.

Assurez-vous que les autorisations accordées à l'utilisateur ou au rôle qui crée la fonction incluent `GetRepositoryPolicySetRepositoryPolicy`,`BatchGetImage`, et`GetDownloadUrlForLayer`.

Par exemple, utilisez la console IAM pour créer un rôle avec la stratégie suivante :

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "ecr:SetRepositoryPolicy",
        "ecr:GetRepositoryPolicy",
        "ecr:BatchGetImage",
```

```
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource": "arn:aws:ecr:us-east-1:111122223333:repository/hello-world"
    }
  ]
}
```

Les autorisations dont Lambda a besoin pour récupérer votre image de conteneur varient selon que le référentiel Amazon ECR se trouve sur le même AWS compte que la fonction ou sur un compte différent. Les sections suivantes expliquent les exigences de chaque scénario.

> **Note**
>
> Dans IAM, l'accès à un même compte ne nécessite qu'une seule partie pour accorder l'autorisation, soit la politique basée sur l'identité (sur le rôle), soit la politique basée sur les ressources (sur le référentiel Amazon ECR). Cross-account l'accès nécessite que les deux parties accordent une autorisation. La politique basée sur l'identité concernant le rôle dans le compte consommateur ET la politique basée sur les ressources du référentiel Amazon ECR du compte propriétaire doivent toutes deux autoriser l'action.

Same-account Politiques relatives aux référentiels Amazon ECR

Pour une fonction associée au même compte que l'image du conteneur dans Amazon ECR, vous pouvez accorder l'accès à Lambda par le biais de la politique basée sur l'identité du rôle d'exécution ou de la politique basée sur les ressources du référentiel Amazon ECR. Un seul côté doit autoriser l'accès.

Si vous choisissez d'utiliser une politique de dépôt Amazon ECR, ajoutez `ecr:BatchGetImage` et `ecr:GetDownloadUrlForLayer` autorisations. L'exemple suivant présente la stratégie minimum :

```
{
        "Sid": "LambdaECRImageRetrievalPolicy",
        "Effect": "Allow",
        "Principal": {
          "Service": "lambda.amazonaws.com"
        },
        "Action": [
          "ecr:BatchGetImage",
          "ecr:GetDownloadUrlForLayer"
```

```
        ]
    }
```

Pour plus d'informations sur les autorisations des référentiels Amazon ECR, consultez Politiques des référentiels privés dans le Guide de l'utilisateur Amazon Elastic Container Registry.

Si le référentiel Amazon ECR n'inclut pas ces autorisations, Lambda tente de les ajouter automatiquement. Lambda ne peut ajouter ces autorisations que si le principal appelant Lambda dispose des autorisations `ecr:getRepositoryPolicy` et `ecr:setRepositoryPolicy`.

Pour afficher ou modifier les autorisations de votre référentiel Amazon ECR, suivez les instructions de la section Définition d'une déclaration de politique de référentiel privé dans le Guide de l'utilisateur Amazon Elastic Container Registry.

Autorisations entre comptes Amazon ECR

Lorsqu'une fonction d'un compte utilise une image de conteneur provenant d'un référentiel Amazon ECR d'un autre compte, les deux parties doivent autoriser l'accès. La politique basée sur l'identité concernant le rôle dans le compte consommateur doit autoriser `ecr:BatchGetImage` et`ecr:GetDownloadUrlForLayer`, et la politique basée sur les ressources du référentiel Amazon ECR du compte propriétaire doit également autoriser ces actions.

Dans l'exemple suivant, votre politique d'autorisations de référentiel Amazon ECR a besoin des instructions suivantes pour accorder l'accès au numéro de compte 123456789012.

- CrossAccountPermission— Permet au compte 123456789012 de créer et de mettre à jour des fonctions Lambda qui utilisent des images provenant de ce référentiel ECR.
- LambdaECRImageCrossAccountRetrievalPolicy— Lambda finit par définir l'état inactif d'une fonction si elle n'est pas invoquée pendant une période prolongée. Cette instruction est requise pour que Lambda puisse récupérer l'image conteneur à des fins d'optimisation et de mise en cache pour le compte de la fonction détenue par 123456789012.

Example– Ajouter une autorisation entre comptes à votre référentiel

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
```

```
    {
      "Sid": "CrossAccountPermission",
      "Effect": "Allow",
      "Action": [
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:root"
      },
      "Resource": "arn:aws:ecr:us-east-1:123456789012:repository/example-lambda-
repository"
    },
    {
      "Sid": "LambdaECRImageCrossAccountRetrievalPolicy",
      "Effect": "Allow",
      "Action": [
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
      "Condition": {
        "ArnLike": {
          "aws:sourceARN": "arn:aws:lambda:us-east-1:123456789012:function:*"
        }
      },
      "Resource": "arn:aws:ecr:us-east-1:123456789012:repository/example-lambda-
repository"
    }
  ]
}
```

Pour donner accès à plusieurs comptes, vous ajoutez les ID de compte à la liste Principal de la stratégie `CrossAccountPermission`et à la liste d'évaluation des conditions dans le`LambdaECRImageCrossAccountRetrievalPolicy`.

Si vous travaillez avec plusieurs comptes au AWS sein d'une organisation, nous vous recommandons d'énumérer chaque ID de compte dans la politique d'autorisation ECR. Cette approche est conforme aux meilleures pratiques de AWS sécurité qui consistent à définir des autorisations restreintes dans les politiques IAM.

Outre la politique de référentiel Amazon ECR, l'utilisateur ou le rôle qui crée la fonction doit également disposer `BatchGetImage` d'`GetDownloadUrlForLayer`autorisations dans sa politique basée sur l'identité.

Cycle de vie des fonctions

Après avoir chargé une nouvelle image de conteneur ou une image de conteneur mise à jour, Lambda optimise l'image avant que la fonction ne puisse traiter les appels. Le processus d'optimisation peut prendre quelques secondes. La fonction reste dans l'état `Pending` jusqu'à ce que le processus se termine, l'état passant alors à `Active`. Vous ne pouvez pas invoquer la fonction jusqu'à ce qu'elle atteigne l'état `Active`.

Si une fonction n'est pas appelée pendant plusieurs semaines, Lambda récupère sa version optimisée, et la fonction passe à l'état `Inactive`. Pour réactiver la fonction, vous devez l'appeler. Lambda rejette la première invocation et la fonction passe à l'état `Pending` jusqu'à ce que Lambda réoptimise l'image. La fonction revient ensuite à l'état `Active`.

Lambda récupère périodiquement l'image de conteneur associée à partir du référentiel Amazon ECR. Si l'image de conteneur correspondante n'existe plus sur Amazon ECR ou si les autorisations ont été révoquées, la fonction passera à l'état `Failed`, et Lambda renverra un message d'échec à tout appel de la fonction.

Vous pouvez utiliser l'API Lambda pour obtenir des informations sur l'état d'une fonction. Pour plus d'informations, consultez États de la fonction d'événement Lambda.

Self-managed Stockage de code S3

Par défaut, lorsque vous créez ou mettez à jour une fonction ou une couche d'événement Lambda à partir d'une archive de fichier .zip, Lambda stocke une copie de votre code dans un espace de stockage. Lambda-managed Chaque AWS compte dispose d'un quota de Lambda-managed stockage de 300 Go par région.

Grâce au stockage de code S3 autogéré, vous pouvez configurer Lambda pour qu'il référence votre code directement à partir d'un compartiment S3 de votre compte. Lambda ne stocke pas de copie de votre code. Le code n'est donc pas pris en compte dans votre quota Lambda-managed de stockage. Lambda accède à votre code directement depuis votre compartiment S3.

Self-managed Le stockage de code S3 est disponible pour toutes les fonctions et couches créées et mises à jour à l'aide d'archives de fichiers .zip. Il est compatible avec toutes les classes de stockage S3 à l'exception des classes de stockage Glacier.

> **Note**
>
> Self-managed Le stockage du code S3 ne modifie pas la taille maximale du package de déploiement .zip, qui reste à 250 Mo (décompressé).

Rubriques

- Configuration du stockage de code S3 autogéré
- Configuration des autorisations
- Création d'une fonction avec un stockage S3 autogéré
- Utilisation d'un stockage S3 autogéré avec couches
- Basculer entre les modes de stockage
- Cycle de vie des fonctions avec stockage autogéré
- Cross-account et utilisation entre régions
- Considérations

Configuration du stockage de code S3 autogéré

Pour utiliser le stockage de code S3 autogéré, procédez comme suit :

1. Créez un compartiment S3 ou utilisez un compartiment existant dans votre compte.
2. Activez le versionnement S3 pour le compartiment. Lambda nécessite la gestion des versions S3 pour suivre la version de votre objet source à utiliser. Chaque fois que vous chargez un nouveau package .zip, S3 crée une nouvelle version afin que Lambda puisse distinguer les mises à jour.
3. Téléchargez votre package de déploiement .zip dans le compartiment S3.
4. Accordez le principal du service Lambda `s3:GetObject` et `s3:GetObjectVersion` les autorisations pour l'objet source. Consultez la section Configuration des autorisations.
5. Créez ou mettez à jour votre fonction ou couche, en spécifiant l'objet S3, la clé S3, la version de l'objet S3 et en le définissant `S3ObjectStorageMode` sur`REFERENCE`.

Configuration des autorisations

Pour utiliser le stockage de code S3 autogéré, accordez au Lambda service principal `lambda.amazonaws.com` () l'autorisation d'accéder à vos objets source. Ajoutez la politique de compartiment S3 suivante :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "LambdaSelfManagedCodeAccess",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource": [
        "arn:aws:s3:::my-bucket/my-function.zip"
      ],
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:lambda:us-east-1:111122223333:function:my-function"
        }
      }
    }
  ]
```

```
}
```

Cette politique de compartiment S3 est distincte du rôle d'exécution de votre fonction. La politique de compartiment est une politique basée sur les ressources qui accorde au Lambda service principal (`lambda.amazonaws.com`) l'autorisation de récupérer un objet de code spécifique afin que Lambda puisse optimiser votre fonction. Il n'accorde aucune autorisation à un autre principal, ni l'autorisation d'invoquer votre fonction. Le rôle d'exécution de votre fonction est une identité IAM distincte que Lambda assume lorsqu'elle exécute votre fonction ; vous accordez des autorisations d'appel et d'autres autorisations d'exécution via les politiques IAM associées à ce rôle. Le fait d'accorder au service Lambda l'accès principal aux objets de votre compartiment n'autorise pas les autres identités à accéder à ces objets ou à invoquer vos fonctions.

Création d'une fonction avec un stockage S3 autogéré

Vous pouvez créer une fonction avec un stockage de code S3 autogéré à l'aide de la console AWS CLI, du ou AWS CloudFormation.

> **Note**
>
> L'éditeur de code de la console Lambda n'est pas disponible pour les fonctions qui utilisent le mode Référence. Pour modifier le code de fonction, mettez à jour le fichier .zip dans votre compartiment S3 et mettez à jour la fonction.

Utilisation de la console

Lorsque vous mettez à jour une fonction depuis un emplacement S3 dans la console Lambda, vous pouvez choisir le mode de stockage du code.

Pour mettre à jour une fonction afin d'utiliser le mode Référence (console)

1. Ouvrez la page Event Functions de la console Lambda.
2. Sélectionnez la fonction à mettre à jour, puis choisissez l'onglet Code.
3. Sous Source du code, choisissez Mettre à jour, puis choisissez Mettre à jour à partir d'un fichier dans Amazon S3.
4. Pour l'URL du lien Amazon S3, entrez l'URL du lien S3 de votre fichier .zip.
5. Sous Mode de stockage du code, choisissez le mode de référence.
6. Cliquez sur Enregistrer.

Après avoir configuré le mode de référence, la section Propriétés du code de l'onglet Code de la fonction affiche le mode de stockage du code : référence et l'emplacement S3 pointant vers votre compartiment S3.

Utilisation de AWS CLI

Utilisez la `create-function` commande avec le `S3ObjectStorageMode=REFERENCE` paramètre :

```
aws lambda create-function \
  --function-name my-function \
  --runtime python3.12 \
  --role arn:aws:iam::111122223333:role/lambda-execution-role \
  --handler lambda_function.lambda_handler \
  --code S3Bucket=my-bucket,\
S3Key=my-function.zip,\
S3ObjectVersion=abc123def456,\
S3ObjectStorageMode=REFERENCE
```

Pour mettre à jour une fonction existante afin d'utiliser le stockage S3 autogéré :

```
aws lambda update-function-code \
  --function-name my-function \
  --s3-bucket my-bucket \
  --s3-key my-function.zip \
  --s3-object-version abc123def456 \
  --s3-object-storage-mode REFERENCE
```

> **⚠ Important**
>
> Vous devez `S3ObjectStorageMode=REFERENCE` le spécifier à chaque appel à`update-function-code`. Si vous omettez`S3ObjectStorageMode`, la valeur par défaut est et `COPY` Lambda stocke votre code dans un espace de stockage. Lambda-managed

Utilisation AWS CloudFormation

Dans votre CloudFormation modèle, définissez `S3ObjectStorageMode` la `Code` propriété `REFERENCE` de la `AWS::Lambda::Function` ressource comme suit :

```
Resources:
```

```
  MyFunction:
    Type: AWS::Lambda::Function
    Properties:
      FunctionName: my-function
      Runtime: python3.12
      Handler: lambda_function.lambda_handler
      Role: !GetAtt LambdaExecutionRole.Arn
      Code:
        S3Bucket: my-bucket
        S3Key: my-function.zip
        S3ObjectVersion: abc123def456
        S3ObjectStorageMode: REFERENCE
```

Utilisation d'un stockage S3 autogéré avec couches

Vous pouvez également utiliser le stockage de code S3 autogéré pour les versions de couches. Utilisez la `publish-layer-version` commande avec `S3ObjectStorageMode=REFERENCE` :

```
aws lambda publish-layer-version \
  --layer-name my-layer \
  --content S3Bucket=my-bucket,S3Key=my-layer.zip,S3ObjectStorageMode=REFERENCE \
  --compatible-runtimes python3.12
```

Vous pouvez utiliser n'importe quelle combinaison de Lambda-managed stockage autogéré pour le code de fonction et le code de couche.

Basculer entre les modes de stockage

Vous pouvez basculer entre Lambda-managed le stockage de code S3 autogéré lorsque vous mettez à jour votre code de fonction ou publiez une nouvelle version de couche. Réglez sur `S3ObjectStorageMode` l'une des valeurs `REFERENCE` suivantes `COPY` ou :

- `COPY`(par défaut) — Lambda copie votre code source dans le stockage. Lambda-managed
- `REFERENCE`— Lambda référence votre code source directement depuis votre compartiment S3 sans en stocker de copie.

Lorsque vous passez de `COPY` à`REFERENCE`, Lambda supprime la Lambda-managed copie de votre code source. Lorsque vous passez de `REFERENCE` à`COPY`, Lambda crée une copie de votre code source dans Lambda-managed le stockage. Le passage à l'`COPY`option échoue si vous dépassez la limite de stockage Lambda-managed du code.

Cycle de vie des fonctions avec stockage autogéré

Lambda accède régulièrement à l'objet source depuis votre compartiment S3 pour réoptimiser votre code de fonction. Vous devez conserver l'accès à l'objet source pour que votre fonction reste active.

- Si Lambda perd l'accès à l'objet source d'une fonction, la fonction passe à l'`Inactive`état. Pour restaurer la fonction, rétablissez l'accès à l'objet source et mettez à jour la fonction.
- Si Lambda perd l'accès à l'objet source d'une couche, la fonction est conservée. `Active` Vous pouvez mettre à jour la configuration des fonctions (sans mettre à jour les couches), mettre à jour le code de fonction ou mettre à jour la configuration des fonctions avec de nouvelles couches. Cependant, la mise à jour de la configuration des fonctions avec la couche inaccessible échoue.

Cross-account et utilisation entre régions

Vous pouvez créer des fonctions et des couches à partir du code source dans des compartiments S3 de différents comptes et de différentes régions. Cross-Region la récupération d'objets entraîne des coûts de transfert de données S3 supplémentaires. Consultez la tarification de S3 pour plus de détails.

Considérations

- Self-managed Le stockage de code S3 est uniquement disponible pour les fonctions et les couches d'archivage de fichiers .zip. Les fonctions d'image de conteneur continuent d'utiliser Amazon ECR.
- La taille maximale du package de déploiement .zip (250 Mo décompressés) reste inchangée.
- Vous payez les tarifs de stockage standard d'Amazon S3 pour le code stocké dans vos buckets autogérés. Lambda ne facture pas la récupération d'objets S3 dans la même région.
- Self-managed Le stockage de code S3 est compatible avec toutes les classes de stockage S3 à l'exception des classes de stockage Glacier.
- Vous pouvez utiliser les fonctionnalités S3 telles que la Cross-Region réplication S3 pour partager des artefacts entre les régions et les politiques de cycle de vie S3 pour gérer les objets.

Configurer la mémoire de la fonction d'événement Lambda

Lambda alloue de la puissance d'UC en fonction de la quantité de mémoire configurée. La mémoire est la quantité de mémoire disponible pour une fonction Lambda lors de l'exécution. Vous pouvez augmenter ou réduire la mémoire et la puissance d'UC allouées à votre fonction à l'aide du paramètre Mémoire. Vous pouvez configurer la mémoire comprise entre 128 et 10 240 Mo, par incréments de 1 Mo. À 1 769 Mo, une fonction possède l'équivalent d'un vCPU (un v CPU-second de crédits par seconde).

Cette page explique comment et quand mettre à jour le paramètre de mémoire pour une fonction Lambda.

Sections

- Évaluation du paramètre de mémoire approprié pour une fonction Lambda
- Configuration de la mémoire d'une fonction (console)
- Configuration de la mémoire des fonctions (AWS CLI)
- Configuration de la mémoire des fonctions (AWS SAM)
- Acceptation des recommandations relatives à la mémoire d'une fonction (console)

Évaluation du paramètre de mémoire approprié pour une fonction Lambda

La mémoire est le principal instrument de contrôle de l'exécution d'une fonction. Le réglage par défaut, 128 Mo, est le plus bas possible. Nous vous recommandons de n'utiliser que 128 Mo pour les fonctions Lambda simples, telles que celles qui transforment et acheminent des événements vers d'autres services AWS .

Une allocation de mémoire plus élevée peut améliorer les performances pour les fonctions qui utilisent des bibliothèques importées, des couches Lambda, Amazon Simple Storage Service (Amazon S3) ou Amazon Elastic File System (Amazon EFS). L'ajout de mémoire augmente proportionnellement la quantité de processeur, augmentant ainsi la puissance de calcul globale disponible. Si une fonction est liée au processeur, au réseau ou à la mémoire, l'augmentation du paramètre de mémoire peut améliorer considérablement ses performances.

Pour trouver la bonne configuration de mémoire, surveillez vos fonctions avec Amazon CloudWatch et configurez des alarmes si la consommation de mémoire approche les valeurs maximales configurées. Cela peut aider à identifier les fonctions liées à la mémoire. Pour CPU-bound et pour IO-bound les fonctions, le suivi de la durée peut également fournir des informations. Dans ces cas,

l'augmentation de la mémoire peut aider à résoudre les goulets d'étranglement de calcul ou de réseau.

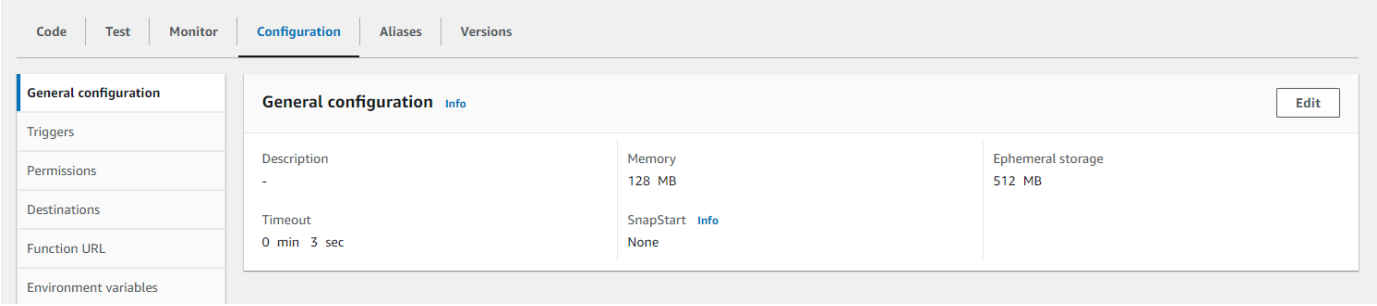
Vous pouvez également envisager d'utiliser l'outil open source AWS Lambda Power Tuning. Cet outil permet AWS Step Functions d'exécuter plusieurs versions simultanées d'une fonction Lambda avec différentes allocations de mémoire et de mesurer les performances. La fonction de saisie s'exécute dans votre AWS compte et effectue des appels HTTP en direct et une interaction avec le SDK, afin de mesurer les performances probables dans un scénario de production en direct. Vous pouvez également implémenter un CI/CD processus permettant d'utiliser cet outil pour mesurer automatiquement les performances des nouvelles fonctions que vous déployez.

Configuration de la mémoire d'une fonction (console)

Vous pouvez configurer la mémoire de votre fonction dans la console Lambda.

Pour mettre à jour la mémoire d'une fonction

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez une fonction.
3. Choisissez Configuration, puis Configuration générale.



4. Sous Configuration générale, choisissez Modifier.
5. Pour Mémoire, définissez une valeur comprise entre 128 et 10 240 Mo.
6. Cliquez sur Enregistrer.

Configuration de la mémoire des fonctions (AWS CLI)

Vous pouvez utiliser la commande update-function-configuration pour configurer la mémoire de votre fonction.

Example

```
aws lambda update-function-configuration \
  --function-name my-function \
  --memory-size 1024
```

Configuration de la mémoire des fonctions (AWS SAM)

Vous pouvez utiliser AWS Serverless Application Model pour configurer la mémoire de votre fonction. Mettez à jour la MemorySizepropriété dans votre `template.yaml` fichier, puis exécutez sam deploy.

Example template.yaml

```
AWSTemplateFormatVersion: '2010-09-09'
Transform: AWS::Serverless-2016-10-31
Description: An AWS Serverless Application Model template describing your function.
Resources:
  my-function:
    Type: AWS::Serverless::Function
    Properties:
      CodeUri: .
      Description: ''
      MemorySize: 1024
      # Other function properties...
```

Acceptation des recommandations relatives à la mémoire d'une fonction (console)

Si vous disposez d'autorisations d'administrateur dans Gestion des identités et des accès AWS (IAM), vous pouvez choisir de recevoir des recommandations de configuration de la mémoire des fonctions Lambda de la part de. Optimiseur de calcul AWS Pour obtenir des instructions sur la manière de choisir de recevoir des recommandations relatives à la mémoire pour votre compte ou votre organisation, consultez Inscription à votre compte dans le Guide de l'utilisateur Optimiseur de calcul AWS .

> **Note**
>
> Compute Optimizer prend en charge uniquement les fonctions qui utilisent l'architecture x86_64.

Si vous avez choisi cette option et si votre fonction Lambda répond aux exigences de Compute Optimizer, vous pouvez afficher et accepter les recommandations de Compute Optimizer relatives à la mémoire de la fonction dans la console Lambda dans Configuration générale.

Configuration du stockage éphémère pour les fonctions d'événements Lambda

Lambda fournit un stockage éphémère pour les fonctions du répertoire `/tmp`. Ce stockage est temporaire et propre à chaque environnement d'exécution. Vous pouvez contrôler la quantité de stockage éphémère allouée à votre fonction à l'aide du paramètre Stockage éphémère. Vous pouvez configurer le stockage éphémère comprise entre 512 et 10 240 Mo, par incréments de 1 Mo. Toutes les données stockées dans `/tmp` sont chiffrées au repos à l'aide d'une clé gérée par AWS.

Cette page décrit les cas d'utilisation courants et explique comment mettre à jour le stockage éphémère pour une fonction Lambda.

Sections

- Cas d'utilisation courants pour un stockage éphémère augmenté
- Configuration du magasin éphémère (console)
- Configuration du stockage éphémère (AWS CLI)
- Configuration du stockage éphémère (AWS SAM)

Cas d'utilisation courants pour un stockage éphémère augmenté

Voici plusieurs cas d'utilisation courants qui bénéficient d'un stockage éphémère augmenté :

- Extract-transform-load Tâches (ETL) : augmentez le stockage éphémère lorsque votre code effectue des calculs intermédiaires ou télécharge d'autres ressources pour terminer le traitement. Un espace temporaire plus important permet d'exécuter des tâches ETL plus complexes dans des fonctions Lambda.
- Inférence de machine learning (ML) : de nombreuses tâches d'inférence reposent sur des fichiers de données de référence volumineux, notamment des bibliothèques et des modèles. Avec un stockage éphémère plus important, vous pouvez télécharger des modèles plus grands depuis Amazon Simple Storage Service (Amazon S3) vers `/tmp` et les utiliser pour votre traitement.
- Traitement des données : pour les charges de travail qui téléchargent des objets depuis Amazon S3 en réponse à des événements S3, un espace `/tmp` plus important permet de gérer des objets plus volumineux sans recourir au traitement en mémoire. Les charges de travail qui créent des PDF ou traitent des médias bénéficient également d'un stockage éphémère plus important.

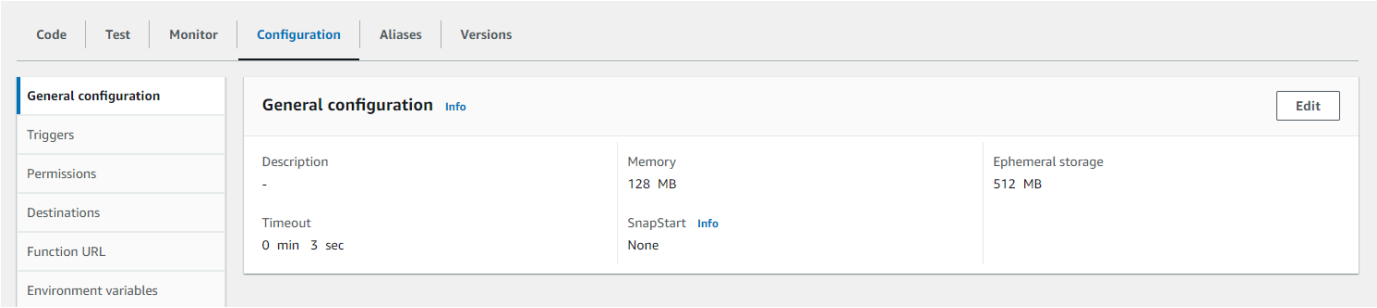
- Traitement graphique : le traitement d'image est un cas d'utilisation courant pour les Lambda-based applications. Pour les charges de travail qui traitent de gros fichiers TIFF ou des images satellites, un stockage éphémère plus important facilite l'utilisation des bibliothèques et l'exécution des calculs dans Lambda.

Configuration du magasin éphémère (console)

Vous pouvez configurer le stockage éphémère dans la console Lambda.

Pour modifier le stockage éphémère d'une fonction

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez une fonction.
3. Choisissez Configuration, puis Configuration générale.



4. Sous Configuration générale, choisissez Modifier.
5. Pour Stockage éphémère, définissez une valeur comprise entre 512 et 10 240 Mo, par incréments de 1 Mo.
6. Cliquez sur Enregistrer.

Configuration du stockage éphémère (AWS CLI)

Vous pouvez utiliser la commande update-function-configuration pour configurer le stockage éphémère.

Example

```
aws lambda update-function-configuration \
  --function-name my-function \
  --ephemeral-storage '{"Size": 1024}'
```

Configuration du stockage éphémère (AWS SAM)

Vous pouvez utiliser AWS Serverless Application Model pour configurer le stockage éphémère pour votre fonction. Mettez à jour la EphemeralStoragepropriété dans votre `template.yaml` fichier, puis exécutez sam deploy.

Example template.yaml

```
AWSTemplateFormatVersion: '2010-09-09'
Transform: AWS::Serverless-2016-10-31
Description: An AWS Serverless Application Model template describing your function.
Resources:
  my-function:
    Type: AWS::Serverless::Function
    Properties:
      CodeUri: .
      Description: ''
      MemorySize: 128
      Timeout: 120
      Handler: index.handler
      Runtime: nodejs22.x
      Architectures:
        - x86_64
      EphemeralStorage:
        Size: 10240
      # Other function properties...
```

Sélection et configuration d’une architecture de jeu d’instructions pour votre fonction Lambda

L'architecture de l'ensemble des instructions d'une fonction Lambda détermine le type de processeur d'ordinateur que Lambda utilise pour exécuter la fonction. Lambda permet de choisir parmi plusieurs architectures de l’ensemble des instructions :

- arm64 — architecture ARM 64 bits, pour AWS Processeurs Graviton.
- x86_64 : architecture 64 bits x86, pour les processeurs x86.

> **Note**
>
> L'architecture arm64 est disponible dans la plupart des Régions AWS. Pour plus d’informations, consultez AWS Lambda Tarification. Dans le tableau des prix de la mémoire, choisissez Prix du bras onglet, puis ouvrez le Région liste déroulante pour voir lequel Régions AWS supporte arm64 avec Lambda.
> Pour un exemple de création d'une fonction avec l'architecture arm64, voir AWS Lambda Fonctions alimentées par AWS Processeur Graviton2.

Rubriques

- Avantages liés à l'utilisation de l'architecture arm64
- Exigences pour la migration vers l'architecture arm64
- Compatibilité des codes de fonction avec l'architecture arm64
- Comment migrer vers l'architecture arm64
- Configuration de l'architecture de l'ensemble des instructions

Avantages liés à l'utilisation de l'architecture arm64

Fonctions Lambda utilisant l'architecture arm64 (AWS Les processeurs Graviton) peuvent atteindre un prix et des performances nettement supérieurs à ceux d'une fonction équivalente exécutée sur une architecture x86_64. Envisagez d'utiliser arm64 pour les applications de calcul intensif telles que le calcul haute performance, le codage vidéo et les applications de simulation.

Lambda gère le matériel sous-jacent et ne garantit pas une génération de processeur spécifique : votre fonction peut s'exécuter sur différentes générations de processeurs Graviton en fonction de la

disponibilité matérielle régionale. Votre code ne cible pas un chipset spécifique ; il doit simplement être compatible avec l'architecture arm64 (AArch64). Toutes les générations de Graviton offrent les avantages suivants par rapport à x86_64 :

- Un cache L2 plus important par processeur virtuel, qui réduit le temps de lecture de la mémoire et améliore la latence pour les backends Web et mobiles, les microservices et les systèmes de traitement des données.
- Performances de chiffrement améliorées grâce aux extensions cryptographiques Arm.
- Prise en charge des jeux d'instructions qui réduisent la latence de CPU-based inférence d'apprentissage automatique.

Pour plus d'informations, voir AWS Processeurs Graviton.

Exigences pour la migration vers l'architecture arm64

Lorsque vous sélectionnez une fonction Lambda à migrer vers l'architecture arm64, pour que la migration soit fluide, assurez-vous que la fonction répond aux exigences suivantes :

- Le package de déploiement ne contient que des composants open source et le code source que vous contrôlez, ce qui vous permet d'effectuer les mises à jour nécessaires à la migration.
- Si le code de la fonction inclut des dépendances tierces, chaque bibliothèque ou package fournit une version arm64.

Compatibilité des codes de fonction avec l'architecture arm64

Le code de la fonction Lambda doit être compatible avec l'architecture de l'ensemble des instructions de la fonction. Avant de migrer une fonction vers l'architecture arm64, veuillez noter les points suivants concernant le code de fonction actuel :

- Si vous avez ajouté le code de la fonction à l'aide de l'éditeur de code intégré, le code s'exécute probablement sur l'une des architectures sans modification.
- Si vous avez chargé le code de la fonction, vous devez charger un nouveau code compatible avec l'architecture cible.
- Si la fonction utilise des couches, vous devez vérifier chaque couche afin de vous assurer qu'elle est compatible avec la nouvelle architecture. Si une couche n'est pas compatible, modifiez la fonction, afin de remplacer la version actuelle de la couche par une version de couche compatible.

- Si la fonction utilise des extensions Lambda, vous devez vérifier chaque extension, afin de vous assurer de sa compatibilité avec la nouvelle architecture.
- Si votre fonction utilise un type de package de déploiement de l'image de conteneur, vous devez créer une nouvelle image de conteneur compatible avec l'architecture de la fonction.

Comment migrer vers l'architecture arm64

Pour migrer une fonction Lambda vers l'architecture arm64, nous recommandons de procéder comme suit :

1. Créez la liste des dépendances de l'application ou de la charge de travail. Les dépendances courantes comprennent :
   - Toutes les bibliothèques et les packages utilisés par la fonction.
   - Les outils que vous utilisez pour créer, déployer et tester la fonction, tels que les compilateurs, les suites de tests, l'intégration continue et la livraison continue (CI/CD) des pipelines, des outils de provisionnement et des scripts.
   - Les extensions Lambda et les outils tiers que vous utilisez pour contrôler la fonction en production.
2. Pour chacune des dépendances, vérifiez la version, puis vérifiez si les versions arm64 sont disponibles.
3. Créez un environnement pour migrer l'application.
4. Amorcez l'application.
5. Testez et déboguez l'application.
6. Testez la performance de la fonction arm64. Comparez la performance avec celle de la version x86_64.
7. Mettez à jour le pipeline d'infrastructure pour prendre en charge les fonctions Lambda arm64.
8. Établissez le déploiement vers la production.

   Par exemple, utilisez la configuration du routage d'alias pour fractionner le trafic entre les versions x86 et arm64 de la fonction et comparez les performances et la latence.

Pour plus d'informations sur la création d'un environnement de code pour l'architecture arm64, y compris des informations spécifiques au langage pour Java, Go, .NET et Python, consultez Commencer avec AWS Graviton GitHub référentiel.

Configuration de l'architecture de l'ensemble des instructions

Vous pouvez configurer l'architecture du jeu d'instructions pour les fonctions Lambda nouvelles et existantes à l'aide de la console Lambda, AWS kits de développement logiciel, AWS Command Line Interface (AWS CLI), ou CloudFormation. Procédez comme suit pour modifier l'architecture de l'ensemble des instructions d'une fonction Lambda existante à partir de la console.

1. Ouvrez le Page des fonctions de l'événement de la console Lambda.
2. Choisissez le nom de la fonction pour laquelle vous voulez configurer l'architecture de l'ensemble des instructions.
3. Dans l'onglet principal Code, pour la section Paramètres d'exécution, choisissez Modifier.
4. Sous Architecture, choisissez l'architecture de l'ensemble des instructions que votre fonction doit utiliser.
5. Cliquez sur Enregistrer.

Configurer le délai d'expiration de la fonction d'événement Lambda

Lambda exécute votre code pendant une durée définie avant l'expiration du délai. Le délai d'expiration est la durée maximale, en secondes, pendant laquelle une fonction Lambda peut être exécutée. La valeur par défaut de ce paramètre est de 3 secondes, mais vous pouvez l'ajuster par incréments d'1 seconde jusqu'à une valeur maximale de 900 secondes (15 minutes).

Pour les fonctions utilisant des instances AWS Lambda gérées, les invocations asynchrones et les invocations de mappage des sources d'événements (sauf Amazon MQ et Amazon DocumentDB) prennent en charge une valeur maximale autorisée de 5 400 secondes (90 minutes).

Cette page explique comment et quand mettre à jour le paramètre de délai d'expiration pour une fonction Lambda.

Sections

- Évaluation de la valeur de délai d'expiration appropriée pour une fonction Lambda
- Configuration du délai d'expiration (console)
- Configuration du délai d'expiration (AWS CLI)
- Configuration du délai d'expiration (AWS SAM)

Évaluation de la valeur de délai d'expiration appropriée pour une fonction Lambda

Si la valeur du délai d'expiration est proche de la durée moyenne d'une fonction, le risque que la fonction expire de façon inattendue est plus élevé. La durée d'une fonction peut varier en fonction de la quantité de données transférées et traitées, ainsi que de la latence des services avec lesquels la fonction interagit. Parmi les causes courantes de délai d'expiration, citons les suivantes :

- Les téléchargements à partir d'Amazon Simple Storage Service (Amazon S3) sont plus importants ou prennent plus de temps que d'habitude.
- Une fonction adresse une requête à un autre service, lequel met plus de temps à répondre.
- Les paramètres fournis à une fonction exigent une plus grande complexité de calcul dans la fonction, ce qui allonge la durée de l'invocation.

Lors des tests de votre application, veillez à ce que ceux-ci reflètent fidèlement la taille et la quantité des données, et à ce que les valeurs des paramètres soient réalistes. Les tests utilisent souvent de petits échantillons pour des raisons de commodité. Cependant, les jeux de données utilisés devraient

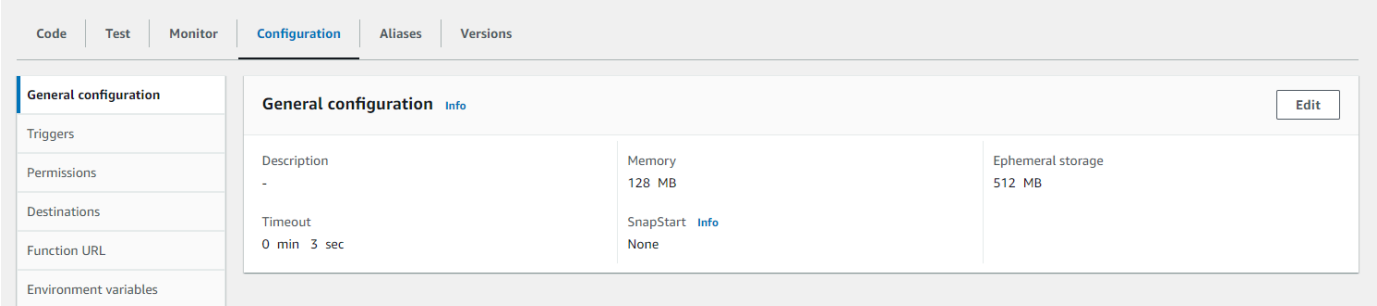
se rapprocher des limites supérieures de ce que l'on peut raisonnablement attendre de votre charge de travail.

Configuration du délai d'expiration (console)

Vous pouvez configurer le délai d'expiration d'une fonction dans la console Lambda.

Pour modifier le délai d'expiration d'une fonction

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez une fonction.
3. Choisissez Configuration, puis Configuration générale.



4. Sous Configuration générale, choisissez Modifier.
5. Pour Expiration, définissez une valeur comprise entre 1 et 900 secondes (15 minutes).
6. Cliquez sur Enregistrer.

Configuration du délai d'expiration (AWS CLI)

Vous pouvez utiliser la commande update-function-configuration pour configurer la valeur du délai d'expiration, en secondes. L'exemple de commande suivant augmente le délai d'expiration de la fonction à 120 secondes (2 minutes).

Example

```
aws lambda update-function-configuration \
  --function-name my-function \
  --timeout 120
```

Configuration du délai d'expiration (AWS SAM)

Vous pouvez utiliser AWS Serverless Application Model pour configurer la valeur du délai d'expiration de votre fonction. Mettez à jour la propriété Timeout dans votre fichier `template.yaml`, puis exécutez sam deploy.

Example template.yaml

```
AWSTemplateFormatVersion: '2010-09-09'
Transform: AWS::Serverless-2016-10-31
Description: An AWS Serverless Application Model template describing your function.
Resources:
  my-function:
    Type: AWS::Serverless::Function
    Properties:
      CodeUri: .
      Description: ''
      MemorySize: 128
      Timeout: 120
      # Other function properties...
```

Utilisation des variables d'environnement Lambda

Vous pouvez utiliser des variables d'environnement pour ajuster le comportement de votre fonction sans mettre à jour le code. Une variable d'environnement est une paire de chaînes stockées dans la configuration spécifique à la version d'une fonction. L'environnement d'exécution de Lambda met les variables d'environnement à la disposition de votre code et définit les variables d'environnement supplémentaires qui contiennent des informations sur la fonction et la demande d'invocation.

> **Note**
>
> Pour renforcer la sécurité, nous vous recommandons d'utiliser à la AWS Secrets Manager place des variables d'environnement pour stocker les informations d'identification de la base de données et d'autres informations sensibles telles que les clés d'API ou les jetons d'autorisation. Pour plus d'informations, consultez Utiliser les secrets de Secrets Manager dans Lambda Event Functions.

Les variables d'environnement ne sont pas évaluées avant l'invocation de la fonction. Toute valeur que vous définissez est considérée comme une chaîne littérale et non développée. Effectuez l'évaluation de la variable dans le code de votre fonction.

Création de variables d'environnement Lambda

Vous pouvez configurer les variables d'environnement dans Lambda à l'aide de la console Lambda, du AWS Command Line Interface (AWS CLI), AWS Serverless Application Model (AWS SAM) ou d'un SDK. AWS

Console

Vous définissez des variables d'environnement sur la version non publiée de votre fonction. Lorsque vous publiez une version, les variables d'environnement sont verrouillées pour cette version ainsi que d'autres paramètres de configuration spécifiques à la version.

Vous créez une variable d'environnement pour votre fonction en définissant une clé et une valeur. Votre fonction utilise le nom de la clé pour récupérer la valeur de la variable d'environnement.

Pour définir des variables d'environnement dans la console Lambda

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez une fonction.

3. Choisissez Configuration, puis Variables d'environnement.
4. Sous Variables d'environnement, choisissez Modifier.
5. Choisissez Ajouter une variable d'environnement.
6. Entrez une clé et une valeur.

   Exigences

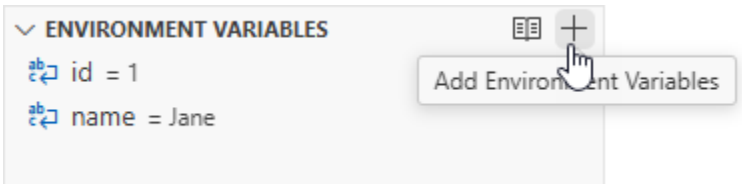
   - Les clés commencent par une lettre et comportent au moins deux caractères.
   - Les clés contiennent uniquement des lettres, des chiffres et le caractère de soulignement (_).
   - Les clés ne sont pas réservées par Lambda.
   - La taille totale de toutes les variables d'environnement ne dépasse pas 4 Ko.
7. Cliquez sur Enregistrer.

Pour générer une liste de variables d'environnement dans l'éditeur de code de la console

Vous pouvez générer une liste de variables d'environnement dans l'éditeur de code Lambda. Il s'agit d'un moyen rapide de référencer vos variables d'environnement pendant que vous codez.

1. Cliquez sur l'onglet Code.
2. Faites défiler l'écran jusqu'à la section VARIABLES D'ENVIRONNEMENT de l'éditeur de code. Les variables d'environnement existantes sont répertoriées ici :

3. Pour créer de nouvelles variables d'environnement, choisissez le signe plus (+) :



Les variables d'environnement restent chiffrées lorsqu'elles sont répertoriées dans l'éditeur de code de la console. Si vous avez activé les assistants de chiffrement pour le chiffrement en

transit, ces paramètres restent inchangés. Pour plus d'informations, consultez Sécurisation de variables d'environnement Lambda.

La liste des variables d'environnement est en lecture seule et n'est disponible que sur la console Lambda. Ce fichier n'est pas inclus lorsque vous téléchargez l'archive .zip de la fonction et vous ne pouvez pas ajouter de variables d'environnement en chargeant ce fichier.

AWS CLI

L'exemple suivant définit deux variables d'environnement sur une fonction nommée `my-function`.

```
aws lambda update-function-configuration \
  --function-name my-function \
  --environment "Variables={BUCKET=amzn-s3-demo-bucket,KEY=file.txt}"
```

Lorsque vous appliquez des variables d'environnement avec la commande `update-function-configuration`, l'ensemble du contenu de la structure `Variables` est remplacé. Pour conserver les variables d'environnement existantes lorsque vous en ajoutez une nouvelle, incluez toutes les valeurs existantes dans votre demande.

Pour obtenir la configuration actuelle, utilisez la commande `get-function-configuration`.

```
aws lambda get-function-configuration \
  --function-name my-function
```

Vous devriez voir la sortie suivante :

```
{
    "FunctionName": "my-function",
    "FunctionArn": "arn:aws:lambda:us-east-2:111122223333:function:my-function",
    "Runtime": "nodejs24.x",
    "Role": "arn:aws:iam::111122223333:role/lambda-role",
    "Environment": {
        "Variables": {
            "BUCKET": "amzn-s3-demo-bucket",
            "KEY": "file.txt"
        }
    },
    "RevisionId": "0894d3c1-2a3d-4d48-bf7f-abade99f3c15",
    ...
```

```
}
```

Vous pouvez transmettre l'identifiant de révision depuis la sortie de `get-function-configuration` en tant que paramètre à `update-function-configuration`. Cela garantit que les valeurs ne changent pas entre le moment où vous lisez la configuration et celui où vous la mettez à jour.

Pour configurer la clé de chiffrement d'une fonction, définissez l'option `KMSKeyARN`.

```
aws lambda update-function-configuration \
  --function-name my-function \
  --kms-key-arn arn:aws:kms:us-east-2:111122223333:key/055efbb4-xmpl-4336-
ba9c-538c7d31f599
```

AWS SAM

Vous pouvez utiliser AWS Serverless Application Model pour configurer les variables d'environnement de votre fonction. Mettez à jour les propriétés Environnement et Variables dans votre fichier `template.yaml`, puis exécutez sam deploy.

Example template.yaml

```
AWSTemplateFormatVersion: '2010-09-09'
Transform: AWS::Serverless-2016-10-31
Description: An AWS Serverless Application Model template describing your function.
Resources:
  my-function:
    Type: AWS::Serverless::Function
    Properties:
      CodeUri: .
      Description: ''
      MemorySize: 128
      Timeout: 120
      Handler: index.handler
      Runtime: nodejs24.x
      Architectures:
        - x86_64
      EphemeralStorage:
        Size: 10240
      Environment:
        Variables:
          BUCKET: amzn-s3-demo-bucket
```

```
            KEY: file.txt
        # Other function properties...
```

AWS SDKs

Pour gérer les variables d'environnement à l'aide d'un AWS SDK, utilisez les opérations d'API suivantes.

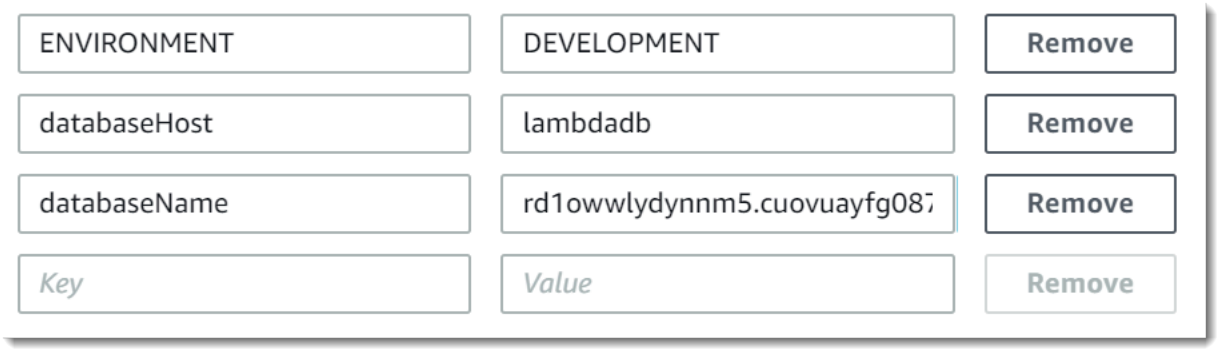
- UpdateFunctionConfiguration
- GetFunctionConfiguration
- CreateFunction

Pour en savoir plus, référez-vous à la documentation du kit SDK AWS correspondant à votre langage de programmation préféré.

Exemple de scénario pour les variables d’environnement

Vous pouvez utiliser des variables d’environnement pour personnaliser le comportement des fonctions dans vos environnements de test et de production. Vous pouvez par exemple créer deux fonctions avec le même code mais une configuration différente. Une fonction se connecte à une base de données de test et l’autre à une base de données de production. Dans ce cas, vous utilisez des variables d’environnement pour transmettre à la fonction le nom d’hôte, ainsi que d’autres détails de connexion pour la base de données.

L’exemple suivant montre comment définir l’hôte de la base de données et le nom de base de données en tant que variables d’environnement.



Si vous souhaitez que votre environnement de test génère plus d’informations de débogage que l’environnement de production, vous pouvez définir une variable d’environnement pour configurer

votre environnement de test de manière à utiliser une journalisation plus approfondie ou un suivi plus détaillé.

Par exemple, dans votre environnement de test, vous pouvez définir une variable d'environnement avec la clé `LOG_LEVEL` et une valeur indiquant le niveau de journalisation du débogage ou du suivi. Dans le code de votre fonction Lambda, vous pouvez ensuite utiliser cette variable d'environnement pour définir le niveau de journalisation.

Les exemples de code suivants en Python Node.js illustrent comment vous pouvez y parvenir. Ces exemples supposent que votre variable d'environnement a une valeur `DEBUG` en Python ou `debug` en Node.js.

Python

Example Code Python pour définir le niveau de journalisation

```
import os
import logging

# Initialize the logger
logger = logging.getLogger()

# Get the log level from the environment variable and default to INFO if not set
log_level = os.environ.get('LOG_LEVEL', 'INFO')

# Set the log level
logger.setLevel(log_level)

def lambda_handler(event, context):
    # Produce some example log outputs
    logger.debug('This is a log with detailed debug information - shown only in test
 environment')
    logger.info('This is a log with standard information - shown in production and
 test environments')
```

Node.js (ES module format)

Example Node.js code pour définir le niveau de journalisation

Cet exemple utilise la bibliothèque de journalisation `winston`. Utilisez npm pour ajouter cette bibliothèque au package de déploiement de votre fonction. Pour plus d'informations, consultez the section called “Création d'un package de déploiement .zip avec dépendances”.

```
import winston from 'winston';

// Initialize the logger using the log level from environment variables, defaulting
 to INFO if not set
const logger = winston.createLogger({
   level: process.env.LOG_LEVEL || 'info',
   format: winston.format.json(),
   transports: [new winston.transports.Console()]
});

export const handler = async (event) => {
   // Produce some example log outputs
   logger.debug('This is a log with detailed debug information - shown only in test
 environment');
   logger.info('This is a log with standard information - shown in production and
 test environment');

};
```

Récupération de variables d'environnement Lambda

Pour récupérer les variables d'environnement dans le code de votre fonction, utilisez la méthode standard pour votre langage de programmation.

Node.js

```
let region = process.env.AWS_REGION
```

Python

```
import os
  region = os.environ['AWS_REGION']
```

> **Note**
>
> Dans certains cas, vous devrez peut-être utiliser le format suivant :
>
> ```
> region = os.environ.get('AWS_REGION')
> ```

Ruby

```
region = ENV["AWS_REGION"]
```

Java

```
String region = System.getenv("AWS_REGION");
```

Go

```
var region = os.Getenv("AWS_REGION")
```

C#

```
string region = Environment.GetEnvironmentVariable("AWS_REGION");
```

PowerShell

```
$region = $env:AWS_REGION
```

Lambda stocke les variables d'environnement en toute sécurité en les chiffrant au repos. Vous pouvez configurer Lambda pour utiliser une clé de chiffrement différente, chiffrer les valeurs des variables d'environnement côté client ou définir des variables d'environnement dans un CloudFormation modèle avec. AWS Secrets Manager

Variables d'environnement d'exécution définies

Les runtimes Lambda définissent plusieurs variables d'environnement lors de l'initialisation. La plupart des variables d'environnement fournissent des informations sur la fonction ou l'exécution. Les clés de ces variables d'environnement sont réservées et ne peuvent pas être définies dans la configuration de la fonction.

Variables d'environnement réservées

- `_HANDLER` – Emplacement de gestionnaire configuré sur la fonction.
- `_X_AMZN_TRACE_ID` – En-tête de suivi X-Ray . Cette variable d'environnement change à chaque invocation.

  - Cette variable d'environnement n'est pas définie pour les environnements d' OS-only exécution (la famille des environnements `provided` d'exécution). Vous pouvez définir `_X_AMZN_TRACE_ID` pour les environnements d'exécution personnalisés à l'aide de l'en-tête de réponse `Lambda-Runtime-Trace-Id` de l'Invocation suivante.
  - Pour les versions 17 et ultérieures du runtime Java, cette variable d'environnement n'est pas utilisée. Lambda stocke plutôt les informations de suivi dans la propriété du système `com.amazonaws.xray.traceHeader`.
- `AWS_DEFAULT_REGION`— L' Région AWS endroit par défaut où la fonction Lambda est exécutée.
- `AWS_REGION`— L' Région AWS endroit où la fonction Lambda est exécutée. Si elle est définie, cette valeur remplace `AWS_DEFAULT_REGION`.
  - Pour plus d'informations sur l'utilisation des variables d' Région AWS environnement avec AWS les SDK, consultez AWS la section Région du Guide de référence AWS des SDK et des outils.
- `AWS_EXECUTION_ENV` – Identifiant d'exécution, doté du préfixe `AWS_Lambda_` (par exemple, `AWS_Lambda_java8`). Cette variable d'environnement n'est pas définie pour les environnements d' OS-only exécution (la famille des environnements `provided` d'exécution).
- `AWS_LAMBDA_FUNCTION_NAME` – Nom de la fonction.
- `AWS_LAMBDA_FUNCTION_MEMORY_SIZE` – Quantité de mémoire disponible pour la fonction en Mo.
- `AWS_LAMBDA_FUNCTION_VERSION` – Version de la fonction en cours d'exécution.
- `AWS_LAMBDA_INITIALIZATION_TYPE`— Le type d'initialisation de la fonction, qui est `on-demand` `provisioned-concurrency`ou`snap-start`, ou`lambda-managed-instances`. Pour plus d'informations, consultez Configuration de la simultanéité provisionnéeAméliorer les performances de démarrage avec Lambda SnapStart, ou. Instances gérées par Lambda
- `AWS_LAMBDA_LOG_GROUP_NAME`, `AWS_LAMBDA_LOG_STREAM_NAME` — Le nom du groupe Amazon CloudWatch Logs et du flux associés à la fonction. Les variables `AWS_LAMBDA_LOG_GROUP_NAME` d'`AWS_LAMBDA_LOG_STREAM_NAME`environnement et ne sont pas disponibles dans les fonctions Lambda SnapStart .
- `AWS_ACCESS_KEY`, `AWS_ACCESS_KEY_ID`, `AWS_SECRET_ACCESS_KEY`, `AWS_SESSION_TOKEN` – Clés d'accès obtenues du rôle d'exécution de la fonction.
- `AWS_LAMBDA_RUNTIME_API` – (exécution personnalisée) Hôte et port de l'API d'exécution..
- `LAMBDA_TASK_ROOT` – Chemin d'accès du code de la fonction Lambda.
- `LAMBDA_RUNTIME_DIR` – Chemin d'accès des bibliothèques de l'environnement d'exécution.

- `AWS_LAMBDA_MAX_CONCURRENCY`— (Instances gérées par Lambda uniquement) Le nombre maximum d'appels simultanés que Lambda enverra à un environnement d'exécution.
- `AWS_LAMBDA_METADATA_API`— L'adresse du serveur de point de terminaison de métadonnées au format `{ipv4_address}:{port}` (par exemple,`169.254.100.1:9001`).
- `AWS_LAMBDA_METADATA_TOKEN`— Un jeton d'authentification unique pour l'environnement d'exécution actuel utilisé pour authentifier les demandes adressées au point de terminaison des métadonnées. Lambda génère ce jeton automatiquement lors de l'initialisation.

Les variables d'environnement supplémentaires suivantes ne sont pas réservées et peuvent être étendues dans la configuration de la fonction.

Variables d'environnement non réservées

- `LANG` – Paramètres régionaux de l'environnement d'exécution (`en_US.UTF-8`).
- `PATH` – Chemin d'exécution (`/usr/local/bin:/usr/bin/:/bin:/opt/bin`).
- `LD_LIBRARY_PATH` – Chemin de la bibliothèque système (`/var/lang/lib:/lib64:/usr/lib64:$LAMBDA_RUNTIME_DIR:$LAMBDA_RUNTIME_DIR/lib:$LAMBDA_TASK_ROOT:$LAMBDA_TASK_ROOT/lib:/opt/lib`).
- `NODE_PATH`— (Node.js) Le chemin Node.js de la bibliothèque (`/opt/nodejs/node12/node_modules/:/opt/nodejs/node_modules:$LAMBDA_RUNTIME_DIR/node_modules`).
- `NODE_OPTIONS`— (Node.js) Pour les Node.js environnements d'exécution, vous pouvez `NODE_OPTIONS` réactiver les fonctionnalités expérimentales que Lambda désactive par défaut.
- `PYTHONPATH` : (Python) le chemin de la bibliothèque Python (`$LAMBDA_RUNTIME_DIR`).
- `GEM_PATH` – (Ruby) Chemin d'accès de la bibliothèque Ruby (`$LAMBDA_TASK_ROOT/vendor/bundle/ruby/3.3.0:/opt/ruby/gems/3.3.0`).
- `AWS_XRAY_CONTEXT_MISSING`— Pour le X-Ray traçage, Lambda le définit pour éviter de `LOG_ERROR` générer des erreurs d'exécution depuis le X-Ray SDK.
- `AWS_XRAY_DAEMON_ADDRESS`— Pour le X-Ray traçage, l'adresse IP et le port du X-Ray démon.
- `AWS_LAMBDA_DOTNET_PREJIT` : (.NET) définissez cette variable pour activer ou désactiver les optimisations d'environnement d'exécution spécifiques à .NET. Les valeurs incluent `always`, `never` et `provisioned-concurrency`. Pour plus d'informations, consultez Configuration de la simultanéité provisionnée pour une fonction événementielle.
- `TZ` – Fuseau horaire de l'environnement (`:UTC`). L'environnement d'exécution utilise NTP pour synchroniser l'horloge système.

Les valeurs d'exemple affichées reflètent les derniers moteurs d'exécution. La présence de variables spécifiques ou leurs valeurs peuvent varier dans les anciens environnements d'exécution.

Sécurisation de variables d'environnement Lambda

Pour sécuriser vos variables d'environnement, vous pouvez utiliser le chiffrement côté serveur pour protéger vos données au repos, et le chiffrement côté client pour protéger vos données en transit.

> **Note**
>
> Pour renforcer la sécurité de la base de données, nous vous recommandons d'utiliser à la AWS Secrets Manager place des variables d'environnement pour stocker les informations d'identification de la base de données. Pour plus d'informations, consultez Utiliser les secrets de Secrets Manager dans Lambda Event Functions.

Sécurité au repos

Lambda fournit toujours le chiffrement côté serveur au repos grâce à une AWS KMS key. Par défaut, Lambda utilise une Clé gérée par AWS. Si ce comportement par défaut convient à votre flux de travail, vous n'avez pas besoin de configurer quoi que ce soit d'autre. Lambda les crée Clé gérée par AWS dans votre compte et gère les autorisations pour vous. AWS l'utilisation de cette clé ne vous est pas facturée.

Si vous préférez, vous pouvez plutôt fournir une clé gérée par le AWS KMS client. Vous pouvez procéder ainsi pour contrôler la rotation de la clé KMS ou pour répondre aux exigences de votre organisation en matière de gestion des clés KMS. Si vous utilisez une clé gérée par le client, seuls les utilisateurs de votre compte ayant accès à la clé KMS peuvent afficher ou gérer les variables d'environnement sur la fonction.

Les clés gérées par le client entraînent des AWS KMS frais standard. Pour en savoir plus, consultez Pricing AWS Key Management Service (Tarification).

Sécurité pendant le transit

Pour plus de sécurité, vous pouvez activer les assistants pour le chiffrement en transit, ce qui garantit que vos variables d'environnement sont chiffrées côté client pour une meilleure protection pendant le transit.

Pour configurer le chiffrement de vos variables d'environnement

1. Utilisez le AWS Key Management Service (AWS KMS) pour créer des clés gérées par le client que Lambda utilisera pour le chiffrement côté serveur et côté client. Pour en savoir plus, consultez Création des clés dans le AWS Key Management Service Guide du développeur .
2. À l'aide de la console Lambda, accédez à la page Modifier les variables d'environnement.
   a. Ouvrez la page Event Functions de la console Lambda.
   b. Choisissez une fonction.
   c. Choisissez Configuration, puis Variables d'environnement dans la barre de navigation de gauche.
   d. Dans la section Variables d'environnement), choisissez Modifier.
   e. Développez Configuration du chiffrement.
3. (Facultatif) Activez les assistants de chiffrement de la console afin qu'ils utilisent le chiffrement côté client pour protéger vos données en transit.
   a. Sous Encryption in transit (Chiffrement pendant le transit), choisissez Enable helpers for encryption in transit (Activer les assistants pour le chiffrement pendant le transit).
   b. Pour chaque variable d'environnement pour laquelle vous souhaitez activer les assistants de chiffrement de la console, choisissez Encrypt (Chiffrer) en regard de la variable d'environnement.
   c. Sous AWS KMS key Pour chiffrer en cours de transfert, choisissez une clé gérée par le client que vous avez créée au début de cette procédure.
   d. Choisissez Politique de rôle d'exécution et copiez la politique. Cette politique octroie au rôle d'exécution de votre fonction l'autorisation de déchiffrer les variables d'environnement.

      Enregistrez cette politique, car vous l'utiliserez à la dernière étape de cette procédure.
   e. Ajoutez le code à votre fonction qui déchiffre les variables d'environnement . Pour obtenir un exemple, choisissez Déchiffrer l'extrait de secrets.
4. (Facultatif) Spécifiez votre clé gérée par le client pour le chiffrement au repos.
   a. Choisissez Utiliser une clé principale client.
   b. Choisissez une clé gérée par le client que vous avez créée au début de cette procédure.
5. Cliquez sur Enregistrer.
6. Configurez des autorisations.

Si vous utilisez une clé gérée par le client avec chiffrement côté serveur, octroyez des autorisations à tous les utilisateurs ou rôles que vous voulez pouvoir afficher ou pour gérer des variables d'environnement sur la fonction. Pour plus d'informations, consultez Gestion des autorisations sur votre clé de chiffrement KMS côté serveur.

Si vous activez le chiffrement côté client pour la sécurité pendant le transit, votre fonction doit disposer d'une autorisation pour appeler l'opération d'API `kms:Decrypt`. Ajoutez la politique que vous avez précédemment enregistrée dans cette procédure au rôle d'exécution de la fonction.

Gestion des autorisations sur votre clé de chiffrement KMS côté serveur

Aucune AWS KMS autorisation n'est requise pour que votre utilisateur ou le rôle d'exécution de la fonction utilise la clé de chiffrement par défaut. Pour utiliser une clé gérée par le client, vous devez disposer des autorisations appropriées pour utiliser la clé. Lambda utilise vos autorisations pour créer un octroi sur la clé. Cela permet à Lambda de l'utiliser pour le chiffrement.

- `kms:ListAliases` – Pour afficher les clés dans la console Lambda.
- `kms:CreateGrant`, `kms:Encrypt` – Pour configurer une clé gérée par le client sur une fonction.
- `kms:Decrypt` – Pour afficher et gérer des variables d'environnement chiffrées à l'aide d'une clé gérée par le client.

Vous pouvez obtenir ces autorisations à partir de votre politique d'autorisation basée sur les ressources Compte AWS ou de celle d'une clé. `ListAliases`est fourni par les politiques gérées pour Lambda. Les stratégies de clé accordent les autorisations restantes aux utilisateurs du groupe Key users (Utilisateurs de clés).

Les utilisateurs sans autorisation `Decrypt` peuvent gérer les fonctions, mais ils ne peuvent pas afficher les variables d'environnement ni les gérer dans la console Lambda. Pour empêcher un utilisateur d'afficher des variables d'environnement, ajoutez une instruction aux autorisations de cet utilisateur afin de refuser l'accès à la clé par défaut, à une clé gérée par le client ou à toutes les clés.

Example Politique IAM – Refuser l'accès en fonction de l'ARN de la clé

JSON

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Deny",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": "arn:aws:kms:us-east-2:111122223333:key/3be10e2d-
xmpl-4be4-bc9d-0405a71945cc"
        }
    ]
}
```

Pour en savoir plus sur la gestion des autorisations de clés, consultez Stratégies de clé dans AWS KMS que vous trouverez dans le Guide du développeur AWS Key Management Service .

Permettre à Lambda Event Functions d'accéder aux ressources d'un Amazon VPC

Avec Amazon Virtual Private Cloud (Amazon VPC), vous pouvez créer des réseaux privés Compte AWS pour héberger des ressources telles que les instances Amazon Elastic Compute Cloud (Amazon EC2), les instances Amazon Relational Database Service (Amazon RDS) et les instances Amazon. ElastiCache Vous pouvez donner à votre fonction Lambda l'accès aux ressources hébergées dans un Amazon VPC en attachant votre fonction au VPC via les sous-réseaux privés qui contiennent les ressources. Suivez les instructions des sections suivantes pour associer une fonction Lambda à un Amazon VPC à l'aide de la console Lambda, du () ou. AWS Command Line Interface AWS CLI AWS SAM

> **Note**
>
> Chaque fonction Lambda s'exécute au sein d'un VPC détenu et géré par le service Lambda. Ces VPC sont gérés automatiquement par Lambda et sont invisibles pour les clients. La configuration de votre fonction pour accéder à d'autres AWS ressources d'un Amazon VPC n'a aucun effet sur le Lambda-managed VPC dans lequel votre fonction s'exécute.

Sections

- Autorisations IAM requises
- Associer des fonctions Lambda à un Amazon VPC dans votre Compte AWS
- Accès à Internet en cas d'attachement à un VPC
- Prise en charge d'IPv6
- Pratiques exemplaires en matière d'utilisation de Lambda avec les Amazon VPC
- Présentation des interfaces interface réseau Elastic (ENI) Hyperplane
- Utilisation des clés de condition IAM pour les paramètres du VPC
- Didacticiels de VPC

Autorisations IAM requises

Pour associer une fonction Lambda à un Amazon VPC dans votre VPC, Compte AWS Lambda a besoin d'autorisations pour créer et gérer les interfaces réseau qu'il utilise pour permettre à votre fonction d'accéder aux ressources du VPC.

Les interfaces réseau créées par Lambda sont interfaces interface réseau Elastic Hyperplane ou ENI Hyperplane. Pour en savoir plus sur ces interfaces réseau, consultez the section called “Présentation des interfaces interface réseau Elastic (ENI) Hyperplane”.

Vous pouvez accorder à votre fonction les autorisations dont elle a besoin en associant la politique AWS gérée AWSLambdaVPCAccessExecutionRoleau rôle d'exécution de votre fonction. Lorsque vous créez une fonction dans la console Lambda et que vous l’associez à un VPC, Lambda ajoute automatiquement cette politique d’autorisations pour vous.

Si vous préférez créer votre propre politique d’autorisations IAM, veillez à inclure toutes les autorisations suivantes et à les autoriser sur toutes les ressources (`"Resource": "*"`) :

- EC2 : CreateNetworkInterface
- EC2 : DescribeNetworkInterfaces
- EC2 : DescribeSubnets
- EC2 : DeleteNetworkInterface
- EC2 : AssignPrivateIpAddresses
- EC2 : UnassignPrivateIpAddresses

Notez que le rôle de votre fonction n’a besoin de ces autorisations que pour créer les interfaces réseau, et non pour invoquer votre fonction. Vous pouvez toujours appeler votre fonction avec succès lorsqu'elle est attachée à un Amazon VPC, même si vous supprimez ces autorisations du rôle d'exécution de votre fonction.

Pour associer votre fonction à un VPC, Lambda doit également vérifier les ressources réseau à l’aide de votre rôle d’utilisateur IAM. Veillez à ce que votre rôle d’utilisateur dispose des autorisations IAM suivantes :

- EC2 : DescribeSecurityGroups
- EC2 : DescribeSubnets
- EC2 : DescribeVpcs
- EC2 : GetSecurityGroupsForVpc

> **Note**
>
> Les autorisations Amazon EC2 que vous accordez au rôle d'exécution de votre fonction sont utilisées par le service Lambda pour associer votre fonction à un VPC. Cependant, ces autorisations sont également accordées implicitement au code de votre fonction. Cela signifie que le code de votre fonction est capable d'effectuer ces appels d'API Amazon EC2. Pour obtenir des conseils sur le respect des pratiques exemplaires en matière de sécurité, consultez the section called "Bonnes pratiques de sécurité".

Associer des fonctions Lambda à un Amazon VPC dans votre Compte AWS

Associez votre fonction à un Amazon VPC dans votre ordinateur à l'aide Compte AWS de la console Lambda, du ou. AWS CLI AWS SAM Si vous utilisez le AWS CLI ou AWS SAM, ou si vous attachez une fonction existante à un VPC à l'aide de la console Lambda, assurez-vous que le rôle d'exécution de votre fonction dispose des autorisations nécessaires répertoriées dans la section précédente.

Les fonctions Lambda ne peuvent pas se connecter directement à un VPC avec la location d'instance dédiée. Pour vous connecter à des ressources dans un VPC dédié, associez-les à un deuxième VPC avec une location par défaut.

Lambda console

Pour attacher une fonction lors de sa création à un Amazon VPC

1. Ouvrez la page Event Functions de la console Lambda et choisissez Create Event Function.
2. Sous Informations de base, dans Nom de fonction, entrez un nom pour votre fonction.
3. Configurez les paramètres VPC pour la fonction en procédant comme suit :
   a. Développez Advanced settings (Paramètres avancés).
   b. Sélectionnez Activer le VPC, puis choisissez le VPC auquel vous souhaitez associer la fonction.
   c. (Facultatif) Pour autoriser le trafic IPv6 sortant, sélectionnez Autoriser le trafic IPv6 pour les sous-réseaux à double pile.
   d. Choisissez les sous-réseaux et les groupes de sécurité pour lesquels créer l'interface réseau. Si vous avez sélectionné Autoriser le trafic IPv6 pour les sous-réseaux à double pile, tous les sous-réseaux sélectionnés doivent avoir un bloc CIDR IPv4 et un bloc CIDR IPv6.

> **Note**
>
> Pour accéder aux ressources privées, connectez votre fonction à des sous-réseaux privés. Si votre fonction a besoin d'un accès Internet, utilisez the section called "Accès Internet pour les fonctions VPC". La connexion d'une fonction à un sous-réseau public ne lui donne pas accès à Internet ou à une adresse IP publique.

4. Choisissez Create Event Function.

Pour associer une fonction existante à un Amazon VPC

1. Ouvrez la page Event Functions de la console Lambda et sélectionnez votre fonction.
2. Choisissez l'onglet Configuration, puis VPC.
3. Choisissez Modifier.
4. Sous VPC, sélectionnez l'Amazon VPC auquel vous souhaitez associer votre fonction.
5. (Facultatif) Pour autoriser le trafic IPv6 sortant, sélectionnez Autoriser le trafic IPv6 pour les sous-réseaux à double pile.
6. Choisissez les sous-réseaux et les groupes de sécurité pour lesquels créer l'interface réseau. Si vous avez sélectionné Autoriser le trafic IPv6 pour les sous-réseaux à double pile, tous les sous-réseaux sélectionnés doivent avoir un bloc CIDR IPv4 et un bloc CIDR IPv6.

> **Note**
>
> Pour accéder aux ressources privées, connectez votre fonction à des sous-réseaux privés. Si votre fonction a besoin d'un accès Internet, utilisez the section called "Accès Internet pour les fonctions VPC". La connexion d'une fonction à un sous-réseau public ne lui donne pas accès à Internet ou à une adresse IP publique.

7. Cliquez sur Enregistrer.

AWS CLI

Pour attacher une fonction lors de sa création à un Amazon VPC

- Pour créer une fonction Lambda et l'attacher à un VPC, exécutez la commande `create-function` de la CLI suivante.

```
aws lambda create-function --function-name my-function \
--runtime nodejs24.x --handler index.js --zip-file fileb://function.zip \
--role arn:aws:iam::123456789012:role/lambda-role \
--vpc-config
 Ipv6AllowedForDualStack=true,SubnetIds=subnet-071f712345678e7c8,subnet-07fd123456788a03
```

Spécifiez vos propres sous-réseaux et groupes de sécurité et configurez `Ipv6AllowedForDualStack` sur `true` ou `false` en fonction de votre cas d'utilisation.

Pour associer une fonction existante à un Amazon VPC

- Pour attacher une fonction existante à un VPC, exécutez la commande `update-function-configuration` de la CLI suivante.

```
aws lambda update-function-configuration --function-name my-function \
--vpc-config Ipv6AllowedForDualStack=true,
 SubnetIds=subnet-071f712345678e7c8,subnet-07fd123456788a036,SecurityGroupIds=sg-085912
```

Pour dissocier votre fonction d'un VPC

- Pour dissocier votre fonction d'un VPC, exécutez la commande `update-function-configuration` de la CLI suivante avec une liste vide de sous-réseaux et de groupes de sécurité VPC.

```
aws lambda update-function-configuration --function-name my-function \
--vpc-config SubnetIds=[],SecurityGroupIds=[]
```

AWS SAM

Pour attacher votre fonction à un VPC

- Pour associer une fonction Lambda à un Amazon VPC, ajoutez la propriété `VpcConfig` à votre définition de fonction, comme illustré par l'exemple de modèle suivant. Pour plus d'informations sur cette propriété, voir AWS: :Lambda : :Function VpcConfig dans le guide de CloudFormation l'utilisateur (la AWS SAM `VpcConfig` propriété est transmise directement à la `VpcConfig` propriété d'une CloudFormation `AWS::Lambda::Function` ressource).

```
AWSTemplateFormatVersion: '2010-09-09'
Transform: AWS::Serverless-2016-10-31

Resources:
  MyFunction:
    Type: AWS::Serverless::Function
    Properties:
      CodeUri: ./lambda_function/
      Handler: lambda_function.handler
      Runtime: python3.12
      VpcConfig:
        SecurityGroupIds:
          - !Ref MySecurityGroup
        SubnetIds:
          - !Ref MySubnet1
          - !Ref MySubnet2
      Policies:
        - AWSLambdaVPCAccessExecutionRole

  MySecurityGroup:
    Type: AWS::EC2::SecurityGroup
    Properties:
      GroupDescription: Security group for Lambda function
      VpcId: !Ref MyVPC

  MySubnet1:
    Type: AWS::EC2::Subnet
    Properties:
      VpcId: !Ref MyVPC
      CidrBlock: 10.0.1.0/24

  MySubnet2:
    Type: AWS::EC2::Subnet
```

```
    Properties:
      VpcId: !Ref MyVPC
      CidrBlock: 10.0.2.0/24

  MyVPC:
    Type: AWS::EC2::VPC
    Properties:
      CidrBlock: 10.0.0.0/16
```

Pour plus d'informations sur la configuration de votre VPC dans AWS SAM, consultez AWS: :EC2 : :VPC dans le guide de l'utilisateur.CloudFormation

Accès à Internet en cas d'attachement à un VPC

Par défaut, les fonctions Lambda ont accès à l'Internet public. Lorsque vous attachez votre fonction à un VPC, son accès est limité aux ressources disponibles au sein de ce VPC. Pour accorder à votre fonction l'accès à Internet, vous devez également configurer le VPC pour qu'il dispose d'un accès à Internet. Pour en savoir plus, consultez the section called "Accès Internet pour les fonctions VPC".

Prise en charge d'IPv6

Votre fonction peut se connecter à des ressources dans des sous-réseaux VPC à double pile via IPv6. Cette option est désactivée par défaut. Pour autoriser le trafic IPv6 sortant, utilisez la console ou l'option `--vpc-config Ipv6AllowedForDualStack=true` avec la commande create-function ou update-function-configuration.

> **Note**
>
> Pour autoriser le trafic IPv6 sortant dans un VPC, tous les sous-réseaux connectés à la fonction doivent être des sous-réseaux à double pile. Lambda ne prend pas en charge les connexions IPv6 sortantes pour les IPv6-only sous-réseaux d'un VPC ni les connexions IPv6 sortantes pour les fonctions qui ne sont pas connectées à un VPC.

Vous pouvez mettre à jour votre code de fonction pour vous connecter explicitement aux ressources du sous-réseau via IPv6. L'exemple Python suivant ouvre un connecteur logiciel et se connecte à un serveur IPv6.

Example— Connexion au serveur IPv6

```
def connect_to_server(event, context):
    server_address = event['host']
    server_port = event['port']
    message = event['message']
    run_connect_to_server(server_address, server_port, message)

def run_connect_to_server(server_address, server_port, message):
    sock = socket.socket(socket.AF_INET6, socket.SOCK_STREAM, 0)
    try:
        # Send data
        sock.connect((server_address, int(server_port), 0, 0))
        sock.sendall(message.encode())
        BUFF_SIZE = 4096
        data = b''
        while True:
            segment = sock.recv(BUFF_SIZE)
            data += segment
            # Either 0 or end of data
            if len(segment) < BUFF_SIZE:
                break
        return data
    finally:
        sock.close()
```

Pratiques exemplaires en matière d’utilisation de Lambda avec les Amazon VPC

Pour vous assurer que votre configuration VPC Lambda est conforme aux pratiques exemplaires en la matière, suivez les conseils des sections suivantes.

Bonnes pratiques de sécurité

Pour associer votre fonction Lambda à un VPC, vous devez accorder au rôle d'exécution de votre fonction un certain nombre d'autorisations Amazon EC2. Ces autorisations sont nécessaires pour créer les interfaces réseau que votre fonction utilise pour accéder aux ressources du VPC. Toutefois, ces autorisations sont également implicitement accordées au code de votre fonction. Cela signifie que le code de votre fonction dispose de l’autorisation d’effectuer ces appels d’API Amazon EC2.

Pour suivre le principe du moindre privilège d'accès, ajoutez une politique de refus, comme dans l'exemple suivant, au rôle d'exécution de votre fonction. Cette politique empêche le code de votre fonction d’appeler les API Amazon EC2, tout en permettant au service

Lambda de gérer les ressources VPC en votre nom. La politique utilise la clé de condition `lambda:SourceFunctionArn`, qui s'applique uniquement aux appels d'API effectués par le code de votre fonction lors de l'exécution. Pour plus d'informations, consultez the section called "ARN de la fonction source".

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                 "ec2:CreateNetworkInterface",
                 "ec2:DeleteNetworkInterface",
                 "ec2:DescribeNetworkInterfaces",
                 "ec2:DescribeSubnets",
                 "ec2:DetachNetworkInterface",
                 "ec2:AssignPrivateIpAddresses",
                 "ec2:UnassignPrivateIpAddresses"
            ],
            "Resource": [ "*" ],
            "Condition": {
                "ArnEquals": {
                    "lambda:SourceFunctionArn": [
                        "arn:aws:lambda:us-
west-2:123456789012:function:my_function"
                    ]
                }
            }
        }
    ]
}
```

AWS fournit des groupes de sécurité et des listes de contrôle d'accès (ACL) réseau pour renforcer la sécurité de votre VPC. Les groupes de sécurité contrôlent le trafic entrant et sortant de vos ressources, et les ACL de réseau contrôlent le trafic entrant et sortant de vos sous-réseaux. Les groupes de sécurité offrent un contrôle d'accès suffisant pour la plupart des sous-réseaux. Vous pouvez utiliser les ACL réseau si vous souhaitez ajouter une couche de sécurité supplémentaire à votre VPC. Pour obtenir des directives générales sur les pratiques exemplaires en matière de

sécurité lors de l'utilisation d'Amazon VPC, consultez Security best practices for your VPC dans le Guide de l'utilisateur Amazon Virtual Private Cloud.

Bonnes pratiques en matière de performances

Lorsque vous attachez votre fonction à un VPC, Lambda vérifie s'il existe une ressource réseau disponible (ENI Hyperplane) à laquelle elle peut se connecter. Les ENI Hyperplane sont associés à une combinaison particulière de groupes de sécurité et de sous-réseaux VPC. Si vous avez déjà attaché une fonction à un VPC, le fait de spécifier les mêmes sous-réseaux et groupes de sécurité lorsque vous attachez une autre fonction signifie que Lambda peut partager les ressources du réseau et éviter d'avoir à créer un nouvel ENI Hyperplane. Pour plus d'informations sur les ENI Hyperplane et leur cycle de vie, consultez the section called "Présentation des interfaces interface réseau Elastic (ENI) Hyperplane".

Présentation des interfaces interface réseau Elastic (ENI) Hyperplane

Une ENI Hyperplane est une ressource gérée qui agit comme une interface réseau entre votre fonction Lambda et les ressources auxquelles vous souhaitez que votre fonction se connecte. Le service Lambda crée et gère ces ENI automatiquement lorsque vous attachez votre fonction à un VPC.

Les ENI d'Hyperplane ne sont pas directement visibles pour vous, et vous n'avez pas besoin de les configurer ou de les gérer. Cependant, le fait de connaître leur fonctionnement peut vous aider à comprendre le comportement de votre fonction lorsque vous l'associez à un VPC.

La première fois que vous attachez une fonction à un VPC à l'aide d'une combinaison particulière de sous-réseau et de groupe de sécurité, Lambda crée une ENI Hyperplane. D'autres fonctions de votre compte qui utilisent la même combinaison de sous-réseau et de groupe de sécurité peuvent également utiliser cette ENI. Dans la mesure du possible, Lambda réutilise les ENI existantes pour optimiser l'utilisation des ressources et minimiser la création d'ENI. Chaque Hyperplane ENI prend en charge jusqu'à 65 connections/ports 000 personnes. Si le nombre de connexions dépasse cette limite, Lambda adapte automatiquement le nombre d'ENI en fonction du trafic réseau et des exigences de simultanéité.

Pour les nouvelles fonctions, pendant que Lambda crée une ENI Hyperplane, votre fonction reste à l'état En attente et vous ne pouvez pas l'invoquer. Votre fonction passe à l'état Actif uniquement lorsque l'ENI Hyperplane est prête, ce qui peut prendre plusieurs minutes. Pour les fonctions existantes, vous ne pouvez pas effectuer d'opérations supplémentaires ciblant la fonction, telles que la création de versions ou la mise à jour du code de la fonction, mais vous pouvez continuer à invoquer les versions précédentes de la fonction.

Dans le cadre de la gestion du cycle de vie de l'ENI, Lambda peut supprimer et recréer les ENI pour équilibrer la charge du trafic réseau entre les ENI ou pour résoudre les problèmes détectés lors des bilans de santé des ENI. Par ailleurs, si une fonction Lambda reste inactive pendant 14 jours, Lambda récupère n'importe toutes les ENI Hyperplane inutilisées et définit l'état de la fonction à `Inactive`. La prochaine tentative d'invocation échouera et la fonction entrera à nouveau dans l'état En attente jusqu'à ce que Lambda termine la création ou l'allocation d'une ENI Hyperplane. Nous vous recommandons de ne pas baser votre conception sur la persistance des ENI.

Lorsque vous mettez à jour une fonction pour supprimer sa configuration VPC, Lambda a besoin de 20 minutes au maximum pour supprimer l'ENI Hyperplane attaché. Lambda ne supprime l'ENI que si aucune autre fonction (ou version de fonction publiée) n'utilise cette ENI Hyperplane.

Lambda s'appuie sur les permissions du rôle d'exécution de la fonction pour supprimer l'ENI Hyperplane. Si vous supprimez le rôle d'exécution avant que Lambda ne supprime l'ENI Hyperplane, Lambda ne pourra pas la supprimer. Vous pouvez effectuer la suppression manuellement.

Utilisation des clés de condition IAM pour les paramètres du VPC

Vous pouvez utiliser des clés de Lambda-specific condition pour les paramètres VPC afin de fournir des contrôles d'autorisation supplémentaires pour vos fonctions Lambda. Par exemple, vous pouvez exiger que toutes les fonctions de votre organisation soient connectées à un VPC. Vous pouvez également spécifier les sous-réseaux et les groupes de sécurité que les utilisateurs de la fonction peuvent et ne peuvent pas utiliser.

Lambda prend également en charge les clés de condition suivantes dans les stratégies IAM :

- lambda : VpcIds — Autoriser ou refuser un ou plusieurs VPC.
- lambda : SubnetIds — Autoriser ou refuser un ou plusieurs sous-réseaux.
- lambda : SecurityGroupIds — Autoriser ou refuser un ou plusieurs groupes de sécurité.

L'API Lambda fonctionne CreateFunctionet UpdateFunctionConfigurationprend en charge ces clés de condition. Pour de plus amples informations sur l'utilisation de clés de condition dans des stratégies IAM, consultez Éléments de politique JSON IAM : Condition dans le Guide de l'utilisateur IAM.

> **Tip**
>
> Si votre fonction inclut déjà une configuration VPC à partir d'une demande d'API précédente, vous pouvez envoyer une demande `UpdateFunctionConfiguration` sans la configuration du VPC.

Exemple de stratégies avec des clés de condition pour les paramètres du VPC

Les exemples suivants montrent comment utiliser les clés de condition pour les paramètres du VPC. Après avoir créé une instruction de politique avec les restrictions souhaitées, ajoutez l'instruction de politique pour l'utilisateur ou le rôle cible.

Assurez-vous que les utilisateurs ne déploient que VPC-connected des fonctions

Pour garantir que tous les utilisateurs ne déploient que VPC-connected des fonctions, vous pouvez refuser les opérations de création et de mise à jour de fonctions qui n'incluent pas d'ID VPC valide.

Notez que l'ID de VPC n'est pas un paramètre d'entrée pour la demande `CreateFunction` ou `UpdateFunctionConfiguration`. Lambda récupère la valeur de l'ID de VPC en fonction des paramètres du sous-réseau et du groupe de sécurité.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceVPCFunction",
      "Action": [
          "lambda:CreateFunction",
          "lambda:UpdateFunctionConfiguration"
       ],
      "Effect": "Deny",
      "Resource": "*",
      "Condition": {
        "Null": {
           "lambda:VpcIds": "true"
        }
      }
```

```
    }
  ]
}
```

Refuser aux utilisateurs l'accès à des VPC, des sous-réseaux ou des groupes de sécurité spécifiques

Pour refuser aux utilisateurs l'accès à des VPC spécifiques, utilisez `StringEquals` pour vérifier la valeur de la condition `lambda:VpcIds`. L'exemple suivant refuse aux utilisateurs l'accès à `vpc-1` et `vpc-2`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "EnforceOutOfVPC",
            "Action": [
                "lambda:CreateFunction",
                "lambda:UpdateFunctionConfiguration"
            ],
            "Effect": "Deny",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "lambda:VpcIds": [
                        "vpc-1",
                        "vpc-2"
                    ]
                }
            }
        }
    ]
}
```

Pour refuser aux utilisateurs l'accès à des sous-réseaux spécifiques, utilisez `StringEquals` pour vérifier la valeur de la condition `lambda:SubnetIds`. L'exemple suivant refuse aux utilisateurs l'accès à `subnet-1` et `subnet-2`.

```
{
      "Sid": "EnforceOutOfSubnet",
      "Action": [
          "lambda:CreateFunction",
          "lambda:UpdateFunctionConfiguration"
       ],
      "Effect": "Deny",
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
            "lambda:SubnetIds": ["subnet-1", "subnet-2"]
        }
      }
    }
```

Pour refuser aux utilisateurs l'accès à des groupes de sécurité spécifiques, utilisez `StringEquals` pour vérifier la valeur de la condition `lambda:SecurityGroupIds`. L'exemple suivant refuse aux utilisateurs l'accès à `sg-1` et `sg-2`.

```
{
      "Sid": "EnforceOutOfSecurityGroups",
      "Action": [
          "lambda:CreateFunction",
          "lambda:UpdateFunctionConfiguration"
       ],
      "Effect": "Deny",
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
            "lambda:SecurityGroupIds": ["sg-1", "sg-2"]
        }
      }
    }
  ]
}
```

Autoriser les utilisateurs à créer et à mettre à jour des fonctions avec des paramètres VPC spécifiques

Pour permettre aux utilisateurs d'accéder à des VPC spécifiques, utilisez `StringEquals` pour vérifier la valeur de la condition `lambda:VpcIds`. L'exemple suivant permet aux utilisateurs d'accéder à `vpc-1` et `vpc-2`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "EnforceStayInSpecificVpc",
            "Action": [
                "lambda:CreateFunction",
                "lambda:UpdateFunctionConfiguration"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "lambda:VpcIds": [
                        "vpc-1",
                        "vpc-2"
                    ]
                }
            }
        }
    ]
}
```

Pour permettre aux utilisateurs d'accéder à des sous-réseaux spécifiques, utilisez `StringEquals` pour vérifier la valeur de la condition `lambda:SubnetIds`. L'exemple suivant permet aux utilisateurs d'accéder à `subnet-1` et `subnet-2`.

```
{
      "Sid": "EnforceStayInSpecificSubnets",
      "Action": [
          "lambda:CreateFunction",
```

```
            "lambda:UpdateFunctionConfiguration"
        ],
        "Effect": "Allow",
        "Resource": "*",
        "Condition": {
          "ForAllValues:StringEquals": {
              "lambda:SubnetIds": ["subnet-1", "subnet-2"]
          }
        }
    }
```

Pour permettre aux utilisateurs d'accéder à des groupes de sécurité spécifiques, utilisez `StringEquals` pour vérifier la valeur de la condition `lambda:SecurityGroupIds`. L'exemple suivant permet aux utilisateurs d'accéder à `sg-1` et `sg-2`.

```
{
      "Sid": "EnforceStayInSpecificSecurityGroup",
      "Action": [
          "lambda:CreateFunction",
          "lambda:UpdateFunctionConfiguration"
      ],
      "Effect": "Allow",
      "Resource": "*",
      "Condition": {
        "ForAllValues:StringEquals": {
            "lambda:SecurityGroupIds": ["sg-1", "sg-2"]
        }
      }
    }
  ]
}
```

Didacticiels de VPC

Dans les didacticiels suivants, vous connectez une fonction Lambda à des ressources dans votre VPC.

- Tutoriel : Utilisation d'une fonction Lambda pour accéder à Amazon RDS dans un Amazon VPC
- Tutoriel : Configuration d'une fonction Lambda pour accéder à Amazon ElastiCache dans un Amazon VPC

Pour connecter votre fonction aux ressources d'un VPC appartenant à un autre Compte AWS, consultez. the section called “Attachement de fonctions aux ressources d’un autre compte”

Donner à Lambda Event Functions l'accès à une ressource d'un Amazon VPC via un autre compte

Vous pouvez donner à votre AWS Lambda fonction l'accès à une ressource d'un Amazon VPC dans Amazon Virtual Private Cloud géré par un autre compte, sans exposer l'un ou l'autre VPC à Internet. Avec ce modèle d'accès, vous pouvez partager des données avec d'autres organisations en utilisant AWS. Grâce à ce modèle d’accès, vous pouvez partager des données entre VPC avec un niveau de sécurité et de performance supérieur à celui d’Internet. Configurez votre fonction Lambda pour utiliser une connexion d’appairage d’Amazon VPC pour accéder à ces ressources.

> **Warning**
>
> Lorsque vous autorisez l’accès entre des comptes ou des VPC, vérifiez que votre plan répond aux exigences de sécurité des organisations qui gèrent ces comptes. Le respect des instructions de ce document affecte le niveau de sécurité de vos ressources.

Dans ce tutoriel, vous connectez deux comptes ensemble à l’aide d’une connexion d’appairage via IPv4. Vous configurez une fonction Lambda qui n’est pas déjà connectée à un Amazon VPC. Vous configurez la résolution DNS pour connecter votre fonction à des ressources qui ne fournissent pas d’adresses IP statiques. Pour adapter ces instructions à d’autres scénarios d’appairage, consultez le Guide d’appairage de VPC.

Conditions préalables

Pour permettre à une fonction Lambda d’accéder à une ressource d’un autre compte, vous devez avoir :

- une fonction Lambda, configurée pour s’authentifier auprès de votre ressource puis lire à partir de celle-ci ;
- une ressource d’un autre compte, tel qu’un cluster Amazon RDS, disponible via Amazon VPC ;
- les informations d’identification du compte de votre fonction Lambda et du compte de votre ressource. Si vous n’êtes pas autorisé à utiliser le compte de votre ressource, contactez un utilisateur autorisé pour préparer ce compte ;
- l’autorisation de créer et de mettre à jour un VPC (et de prendre en charge les ressources Amazon VPC) à associer à votre fonction Lambda ;
- l’autorisation de mettre à jour le rôle d’exécution et la configuration VPC de votre fonction Lambda ;

- l’autorisation de créer une connexion d’appairage de VPC dans le compte de votre fonction Lambda ;
- l’autorisation d’accepter une connexion d’appairage de VPC dans le compte de votre ressource ;
- l’autorisation de mettre à jour la configuration du VPC de votre ressource (et de prendre en charge les ressources Amazon VPC) ;
- l’autorisation d’invoquer votre fonction Lambda.

Création d’un Amazon VPC dans le compte de votre fonction

Créez un Amazon VPC, des sous-réseaux, des tables de routage et un groupe de sécurité dans le compte de votre fonction Lambda.

Pour créer un VPC, des sous-réseaux et d'autres ressources VPC à l'aide de la console

1. Ouvrez la console Amazon VPC à l’adresse https://console.aws.amazon.com/vpc/.
2. Sur le tableau de bord, choisissez Créer un VPC.
3. Pour le bloc d’adresse CIDR IPv4, fournissez un bloc d’adresse CIDR privé. Votre bloc d’adresse CIDR ne doit chevaucher aucun bloc utilisé dans le VPC de votre ressource. Ne choisissez ni un bloc que le VPC de vos ressources utilise pour attribuer des adresses IP aux ressources, ni un bloc déjà défini dans les tables de routage de votre VPC de ressources. Pour plus d’informations sur la définition des blocs d’adresse CIDR appropriés, consultez VPC CIDR blocks.
4. Choisissez Personnaliser les zones de disponibilité.
5. Sélectionnez les mêmes zones de disponibilité que votre ressource.
6. Pour Nombre de sous-réseaux publics, choisissez 0.
7. Pour VPC endpoints (Points de terminaison d'un VPC), choisissez None (Aucun).
8. Sélectionnez Create VPC (Créer un VPC).

Octroi d’autorisations VPC au rôle d’exécution de votre fonction

AWSLambdaVPCAccessExecutionRoleAttachez-vous au rôle d'exécution de votre fonction pour lui permettre de se connecter aux VPC.

Pour octroyer des autorisations VPC au rôle d’exécution de votre fonction

1. Ouvrez la page Event Functions de la console Lambda.

2. Choisissez le nom de votre fonction .
3. Choisissez Configuration.
4. Choisissez Autorisations.
5. Sous Nom du rôle, choisissez le rôle d'exécution.
6. Dans la section Politiques d'autorisations, choisissez Ajouter des autorisations.
7. Dans la liste déroulante, choisissez Attacher des politiques.
8. Dans la zone de recherche, saisissez `AWSLambdaVPCAccessExecutionRole`.
9. À gauche du nom de politique, cochez la case.
10. Choisissez Ajouter des autorisations.

Pour attacher votre fonction à votre Amazon VPC

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez le nom de votre fonction .
3. Choisissez l'onglet Configuration, puis VPC.
4. Choisissez Modifier.
5. Sous VPC, sélectionnez votre VPC.
6. Sous Sous-réseaux, choisissez vos sous-réseaux.
7. Sous Groupe de sécurité, sélectionnez le groupe de sécurité par défaut de votre VPC.
8. Cliquez sur Enregistrer.

Création d'une requête de connexion d'appairage de VPC

Créez une requête de connexion d'appairage de VPC entre le VPC de votre fonction (le VPC demandeur) et le VPC de votre ressource (le VPC accepteur).

Pour demander une connexion d'appairage de VPC depuis le VPC de votre fonction

1. Ouvrez la https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Peering connections (Connexions d'appairage).
3. Choisissez Create peering connection (Créer une connexion d'appairage).
4. Pour ID VPC (demandeur), sélectionnez le VPC de votre fonction.
5. Pour ID de compte, saisissez l'ID du compte de votre ressource.

6. Pour VPC ID (Accepter), saisissez le VPC de votre ressource.

Préparation du compte de votre ressource

Pour créer votre connexion d'appairage et préparer le VPC de votre ressource à utiliser la connexion, connectez-vous au compte de votre ressource avec un rôle doté des autorisations répertoriées dans les conditions requises. Les étapes de connexion peuvent être différentes en fonction de la manière dont le compte est sécurisé. Pour plus d'informations sur la connexion à un AWS compte, consultez le guide de l'AWS Sign-in utilisateur. Au sein du compte de votre ressource, effectuez les procédures suivantes.

Pour accepter une requête de connexion d'appairage de VPC

1. Ouvrez la https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Peering connections (Connexions d'appairage).
3. Sélectionnez la connexion d'appairage de VPC en attente (statut pending-acceptance).
4. Choisissez Actions.
5. Dans la liste déroulante Actions, choisissez Accepter la demande.
6. Lorsque vous êtes invité à confirmer l'opération, choisissez Accepter la demande.
7. Choisissez Modifier mes tables de routage maintenant pour ajouter une route à la table de routage principale de votre VPC afin de pouvoir envoyer et recevoir du trafic via la connexion d'appairage.

Inspectez les tables de routage du VPC de la ressource. La route générée par Amazon VPC peut ne pas établir de connectivité, en fonction de la configuration du VPC de votre ressource. Vérifiez les conflits entre la nouvelle route et la configuration existante du VPC. Pour plus d'informations sur le dépannage, consultez Troubleshoot a VPC peering connection dans le Guide d'appairage de VPC Amazon Virtual Private Cloud.

Pour mettre à jour le groupe de sécurité de votre ressource

1. Ouvrez la https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Groupes de sécurité.
3. Sélectionnez le groupe de sécurité pour votre ressource.
4. Choisissez Actions.

5. Dans la liste déroulante, choisissez Modifier les règles entrantes.
6. Choisissez Ajouter une règle.
7. Pour Source, entrez l'ID de compte et l'ID de groupe de sécurité de votre fonction, séparés par une barre oblique (par exemple, 111122223333/sg -1a2b3c4d).
8. Choisissez Edit outbound rules (Modifier les règles sortantes).
9. Vérifiez si le trafic sortant est restreint. Les paramètres de VPC par défaut autorisent tout le trafic sortant. Si le trafic sortant est restreint, passez à l'étape suivante.
10. Choisissez Ajouter une règle.
11. Pour Destination, entrez l'ID de compte et l'ID de groupe de sécurité de votre fonction, séparés par une barre oblique (par exemple, 111122223333/sg -1a2b3c4d).
12. Sélectionnez Enregistrer les règles.

Pour activer la résolution DNS pour votre connexion d'appairage

1. Ouvrez la https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Peering connections (Connexions d'appairage).
3. Sélectionnez votre connexion d'appairage.
4. Choisissez Actions.
5. Choisissez Modifier les paramètres DNS.
6. En-dessous de Résolution DNS acceptée, sélectionnez Autoriser le VPC demandeur à convertir le DNS des hôtes VPC accepteurs en IP privée.
7. Cliquez sur Enregistrer les modifications.

Mise à jour de la configuration VPC dans le compte de votre fonction

Connectez-vous au compte de votre fonction, puis mettez à jour la configuration du VPC.

Pour ajouter une route pour une connexion d'appairage de VPC

1. Ouvrez la https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Route tables (Tables de routage).
3. Cochez la case en regard du nom de la table de routage pour le sous-réseau que vous avez associé à votre fonction.

4. Choisissez Actions.
5. Choisissez Edit routes (Modifier des routes).
6. Choisissez Ajouter une route.
7. Pour Destination, saisissez le bloc CIDR du VPC de votre ressource.
8. Pour Cible, sélectionnez la connexion d'appairage de VPC.
9. Cliquez sur Enregistrer les modifications.

Pour plus d'informations sur les considérations que vous pourriez rencontrer lors de la mise à jour de vos tables de routage, consultez Mettre à jour vos tables de routage pour une connexion d'appairage VPC.

Pour mettre à jour le groupe de sécurité de votre fonction Lambda

1. Ouvrez la https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Groupes de sécurité.
3. Choisissez Actions.
4. Choisissez Modifier les règles entrantes.
5. Choisissez Ajouter une règle.
6. Pour Source, entrez l'ID de compte et l'ID de groupe de sécurité de votre ressource, séparés par une barre oblique (par exemple, 111122223333/sg -1a2b3c4d).
7. Sélectionnez Enregistrer les règles.

Pour activer la résolution DNS pour votre connexion d'appairage

1. Ouvrez la https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Peering connections (Connexions d'appairage).
3. Sélectionnez votre connexion d'appairage.
4. Choisissez Actions.
5. Choisissez Modifier les paramètres DNS.
6. Sous Résolution DNS du demandeur, sélectionnez Autoriser le VPC accepteur à convertir le DNS des hôtes VPC demandeur en IP privée.
7. Cliquez sur Enregistrer les modifications.

Test de votre fonction

Pour créer un événement de test et inspecter la sortie de votre fonction

1. Dans le volet Source du code, choisissez Test.
2. Sélectionnez Créer un événement.
3. Dans le panneau JSON d'événement, remplacez les valeurs par défaut par une entrée adaptée à votre fonction Lambda.
4. Sélectionnez Invoquer .
5. Dans l'onglet Résultats de l'exécution, vérifiez que Response contient le résultat attendu.

En outre, vous pouvez consulter les journaux de votre fonction pour vérifier qu'ils correspondent à vos attentes.

Pour consulter les enregistrements d'invocation de votre fonction dans Logs CloudWatch

1. Choisissez l'onglet Surveiller.
2. Choisissez Afficher CloudWatch les journaux.
3. Dans l'onglet Flux de journaux, choisissez le flux de journaux pour l'invocation de votre fonction.
4. Vérifiez que vos journaux sont conformes à vos attentes.

Activer l'accès à Internet pour les fonctions VPC-connected d'événement Lambda

Par défaut, les fonctions Lambda s'exécutent dans un Lambda-managed VPC disposant d'un accès Internet. Pour accéder aux ressources d’un VPC dans votre compte, vous pouvez ajouter une configuration VPC à une fonction. Cela limite la fonction aux ressources de ce VPC, sauf si le VPC dispose d’un accès à Internet. Cette page explique comment fournir un accès Internet aux fonctions VPC-connected Lambda.

Je n’ai pas encore de VPC

Créer le VPC

Le flux de travail de création de VPC crée toutes les ressources VPC requises pour qu’une fonction Lambda accède à l’Internet public à partir d’un sous-réseau privé, y compris les sous-réseaux, la passerelle NAT, la passerelle Internet et les entrées de table de routage.

Pour créer le VPC

1. Ouvrez la console Amazon VPC à l’adresse https://console.aws.amazon.com/vpc/.
2. Sur le tableau de bord, choisissez Créer un VPC.
3. Sous Ressources à créer, choisissez VPC et plus encore.
4. Configurer le VPC
    a. Pour Name tag auto-generation (Génération automatique de balises de nom), saisissez un nom pour le VPC.
    b. Pour Bloc d'adresse CIDR IPv4, vous pouvez conserver la suggestion par défaut ou saisir le bloc d'adresse CIDR requis par votre application ou votre réseau.
    c. Si votre application communique en utilisant des adresses IPv6, choisissez le bloc d'adresse CIDR IPv6, le bloc Amazon-provided d'adresse CIDR IPv6.
5. Configurer les sous-réseaux
    a. Pour Nombre de zones de disponibilité, choisissez 2. Nous recommandons au moins deux zones de disponibilité pour une haute disponibilité.
    b. Pour Number of public subnets (Nombre de sous-réseaux publics), choisissez 2.
    c. Pour Number of private subnets (Nombre de sous-réseaux privés), choisissez 2.

d. Vous pouvez conserver le bloc d'adresse CIDR par défaut pour le sous-réseau public ou développer Personnaliser les blocs d'adresse CIDR du sous-réseau et saisir un bloc d'adresse CIDR. Pour plus d'informations, consultez Subnet CIDR blocks.

6. Pour Passerelles NAT, choisissez 1 par zone de disponibilité afin d'améliorer la résilience.
7. Pour Passerelle Internet de sortie uniquement, choisissez Oui si vous avez choisi d'inclure un bloc d'adresse CIDR IPv6.
8. Pour Points de terminaison de VPC, conservez la valeur par défaut (Passerelle S3). Cette option n'entraîne pas de frais. Pour plus d'informations, consultez Types of VPC endpoints for Amazon S3.
9. Pour Options DNS, conservez les paramètres par défaut.
10. Sélectionnez Create VPC (Créer un VPC).

Configurer la fonction Lambda

Pour configurer un VPC lorsque vous créez une fonction

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez Create Event Function.
3. Sous Informations de base, dans Nom de fonction, entrez un nom pour votre fonction.
4. Développez Advanced settings (Paramètres avancés).
5. Sélectionnez Activer le VPC, puis choisissez un VPC.
6. (Facultatif) Pour autoriser le trafic IPv6 sortant, sélectionnez Autoriser le trafic IPv6 pour les sous-réseaux à double pile.
7. Pour Sous-réseaux, sélectionnez tous les sous-réseaux privés. Les sous-réseaux privés peuvent accéder à Internet via une passerelle NAT. La connexion d'une fonction à un sous-réseau public ne lui donne pas accès à Internet.

> **Note**
>
> Si vous avez sélectionné Autoriser le trafic IPv6 pour les sous-réseaux à double pile, tous les sous-réseaux sélectionnés doivent avoir un bloc CIDR IPv4 et un bloc CIDR IPv6.

8. Pour les groupes de sécurité, sélectionnez un groupe de sécurité qui autorise le trafic sortant.

9. Choisissez Create Event Function.

Lambda crée automatiquement un rôle d'exécution avec la politique AWSLambdaVPCAccessExecutionRole AWS gérée. Les autorisations de cette politique ne sont nécessaires que pour créer des interfaces réseau élastiques pour la configuration VPC, et non pour invoquer votre fonction. Pour appliquer les autorisations de moindre privilège, vous pouvez supprimer la AWSLambdaVPCAccessExecutionRolepolitique de votre rôle d'exécution après avoir créé la fonction et la configuration VPC. Pour plus d'informations, consultez Autorisations IAM requises.

Pour configurer un VPC pour une fonction existante

Pour ajouter une configuration VPC à une fonction existante, le rôle d'exécution de la fonction doit être autorisé à créer et à gérer des interfaces réseau élastiques. La politique AWSLambdaVPCAccessExecutionRole AWS gérée inclut les autorisations requises. Pour appliquer les autorisations de moindre privilège, vous pouvez supprimer la AWSLambdaVPCAccessExecutionRolepolitique de votre rôle d'exécution après avoir créé la configuration VPC.

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez une fonction.
3. Choisissez l'onglet Configuration puis choisissez VPC.
4. Sous VPC, choisissez Modifier.
5. Sélectionnez le VPC.
6. (Facultatif) Pour autoriser le trafic IPv6 sortant, sélectionnez Autoriser le trafic IPv6 pour les sous-réseaux à double pile.
7. Pour Sous-réseaux, sélectionnez tous les sous-réseaux privés. Les sous-réseaux privés peuvent accéder à Internet via une passerelle NAT. La connexion d'une fonction à un sous-réseau public ne lui donne pas accès à Internet.

   > **Note**
   >
   > Si vous avez sélectionné Autoriser le trafic IPv6 pour les sous-réseaux à double pile, tous les sous-réseaux sélectionnés doivent avoir un bloc CIDR IPv4 et un bloc CIDR IPv6.

8. Pour les groupes de sécurité, sélectionnez un groupe de sécurité qui autorise le trafic sortant.

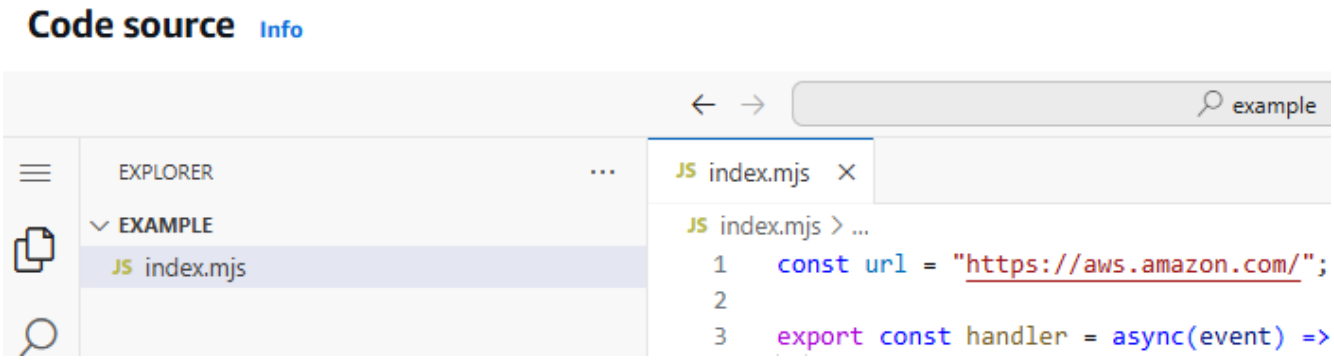
9. Cliquez sur Enregistrer.

Tester la fonction

Utilisez l'exemple de code suivant pour vérifier que votre VPC-connected fonction peut accéder à l'Internet public. En cas de succès, le code renvoie un code d'état `200`. En cas d'échec, la fonction expire.

Node.js

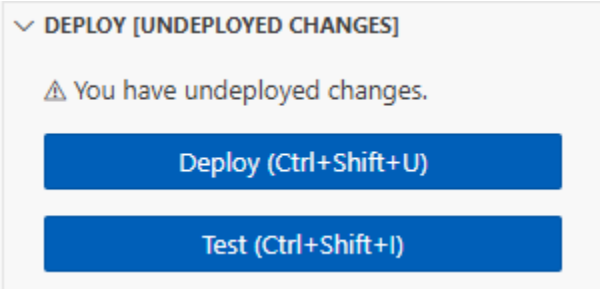
1. Dans le volet Source du code de la console Lambda, collez le code suivant dans le fichier index.mjs. La fonction envoie une requête HTTP GET à un point de terminaison public et renvoie le code de réponse HTTP pour tester si la fonction a accès à l'Internet public.



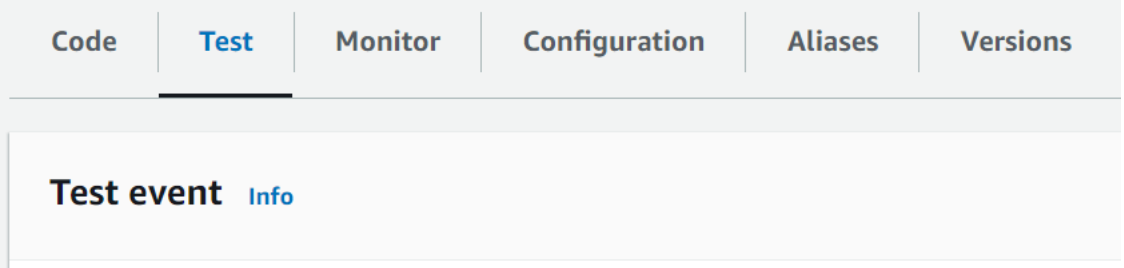
   Example— Requête HTTP avec async/await

```
const url = "https://aws.amazon.com/";

export const handler = async(event) => {
    try {
        const res = await fetch(url);
        console.info("status", res.status);
        return res.status;
    }
    catch (e) {
        console.error(e);
        return 500;
    }
};
```

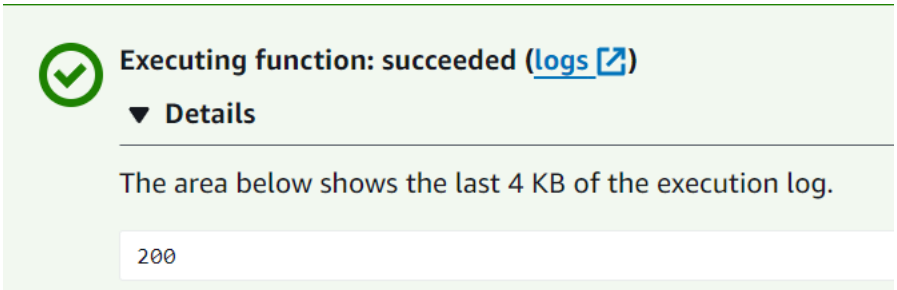
2. Dans la section DÉPLOYER, choisissez Déployer pour mettre à jour le code de votre fonction :



3. Choisissez l'onglet Test.



4. Sélectionnez Tester).
5. La fonction renvoie un code d'état `200`. Cela signifie que la fonction dispose d'un accès Internet sortant.



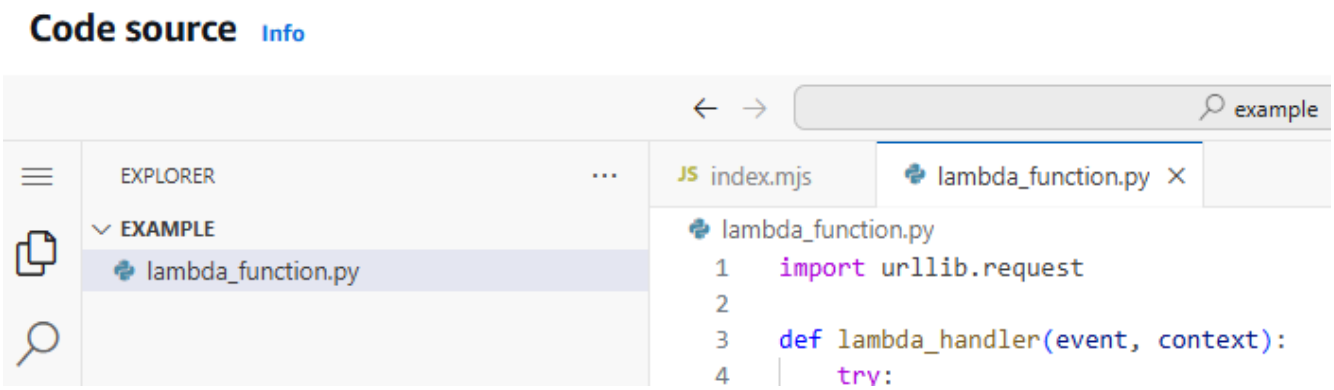
Si la fonction ne parvient pas à accéder à l'Internet public, un message d'erreur de ce type s'affiche :

```
{
  "errorMessage": "2024-04-11T17:22:20.857Z abe12jlc-640a-8157-0249-9be825c2y110
 Task timed out after 3.01 seconds"
}
```

Python

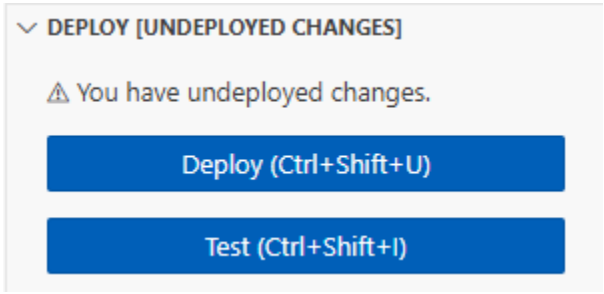
1. Dans le volet Source du code de la console Lambda, collez le code suivant dans le fichier lambda_function.py. La fonction envoie une requête HTTP GET à un point de terminaison

public et renvoie le code de réponse HTTP pour tester si la fonction a accès à l'Internet public.

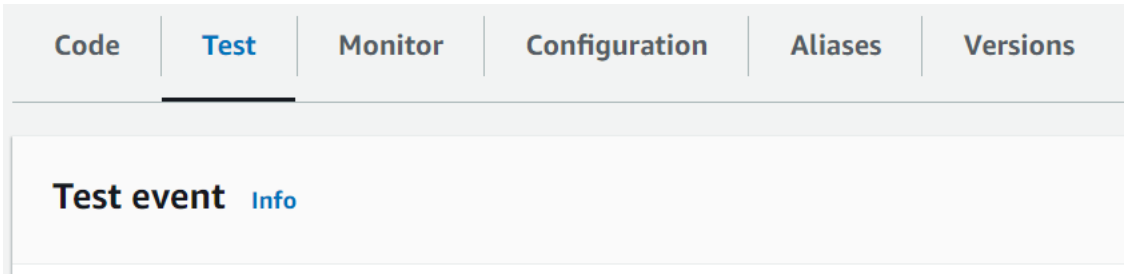



```
import urllib.request

def lambda_handler(event, context):
    try:
        response = urllib.request.urlopen('https://aws.amazon.com')
        status_code = response.getcode()
        print('Response Code:', status_code)
        return status_code
    except Exception as e:
        print('Error:', e)
        raise e
```

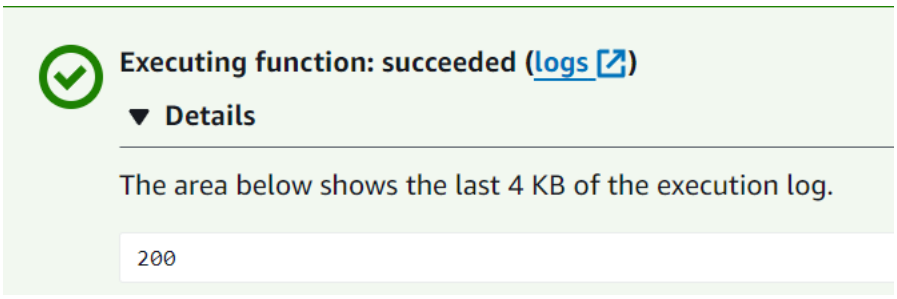
2. Dans la section DÉPLOYER, choisissez Déployer pour mettre à jour le code de votre fonction :



3. Choisissez l'onglet Test.



4. Sélectionnez Tester).
5. La fonction renvoie un code d'état `200`. Cela signifie que la fonction dispose d'un accès Internet sortant.



Si la fonction ne parvient pas à accéder à l'Internet public, un message d'erreur de ce type s'affiche :

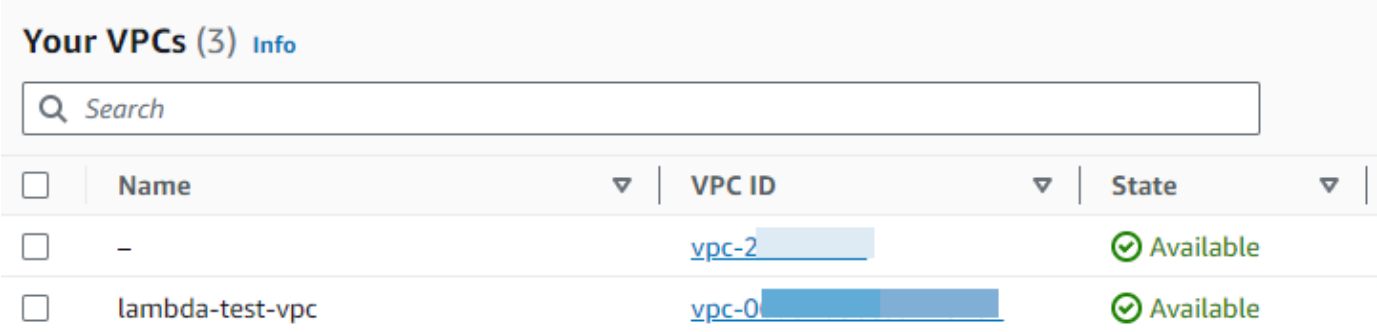
```
{
  "errorMessage": "2024-04-11T17:22:20.857Z abe12jlc-640a-8157-0249-9be825c2y110
 Task timed out after 3.01 seconds"
}
```

J'ai déjà un VPC

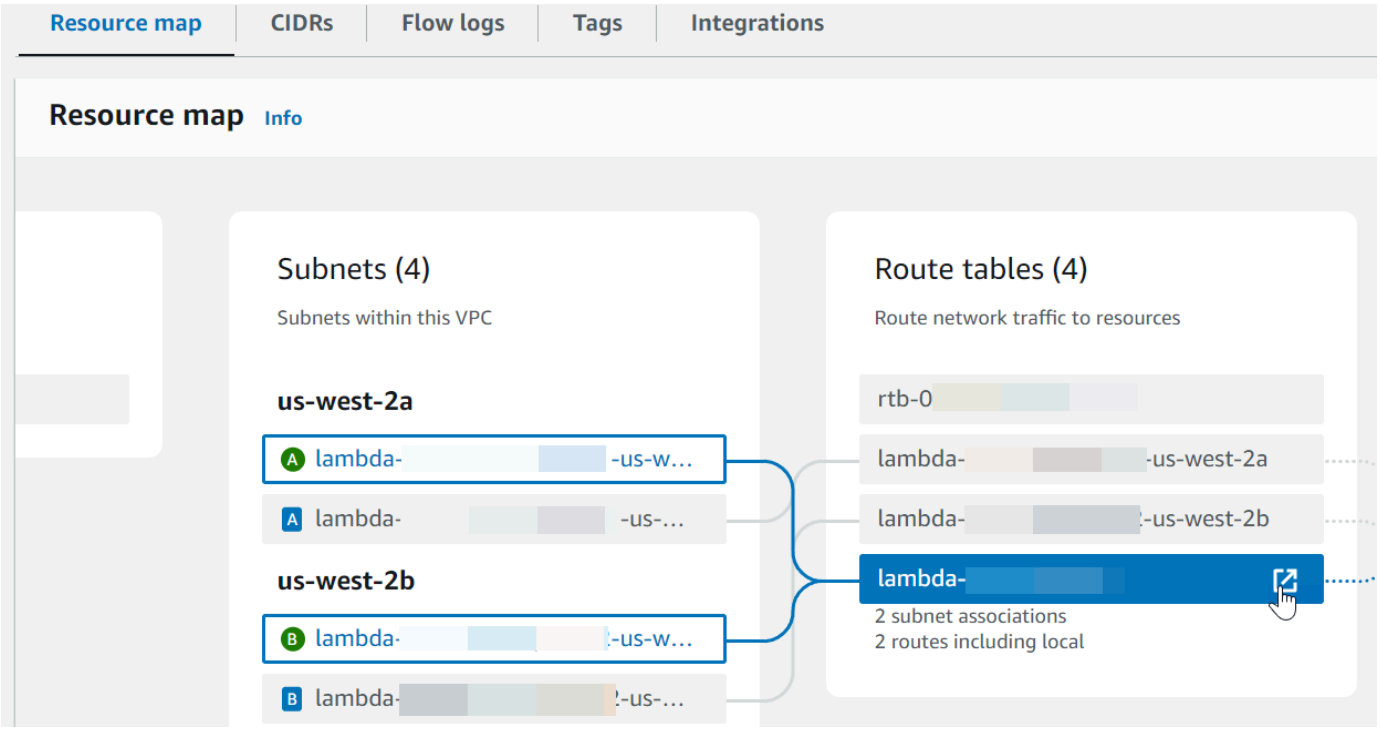
Si vous possédez déjà un VPC mais que vous devez configurer un accès Internet public pour une fonction Lambda, procédez comme suit. Cette procédure suppose que votre VPC possède au moins deux sous-réseaux. Si vous n'avez pas deux sous-réseaux, consultez Create a subnet dans le Guide de l'utilisateur Amazon VPC.

Vérification de la configuration de la table de routage

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Choisissez l'ID de VPC.



3. Faites défiler la page jusqu'à la section Carte des ressources. Notez les mappages des tables de routage. Ouvrez chaque table de routage mappée à un sous-réseau.

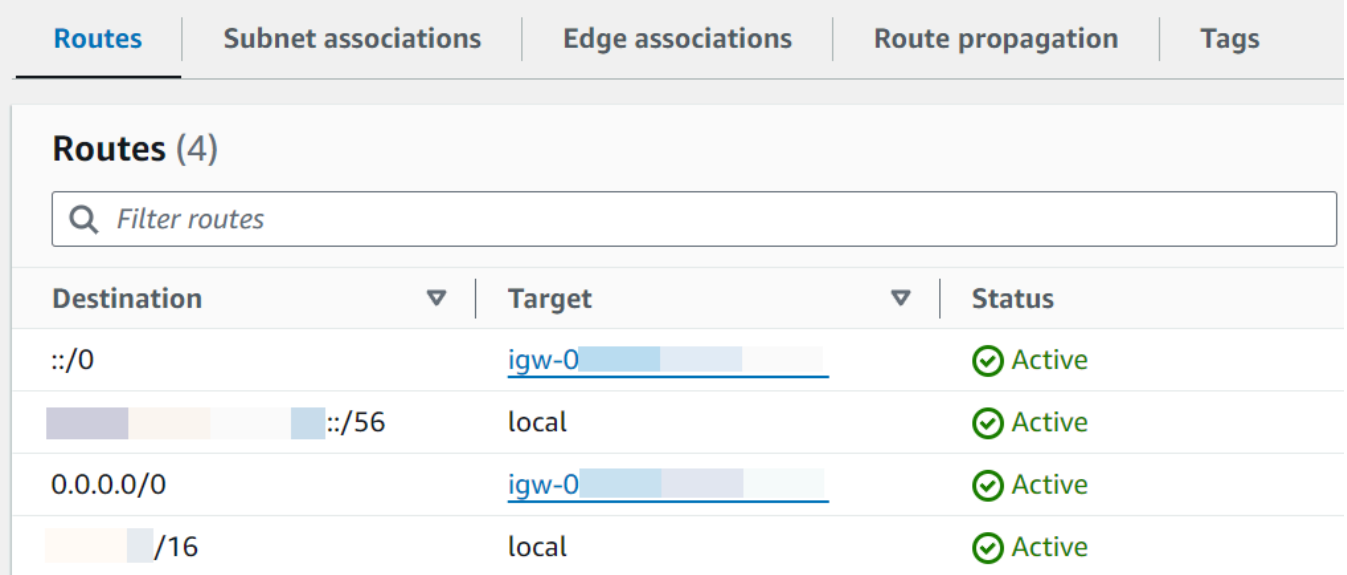


4. Faites défiler jusqu'à l'onglet Routes. Passez en revue les itinéraires pour déterminer si votre VPC possède les deux tables de routage suivantes. Chacune de ces exigences doit être satisfaite par une table de routage distincte.

   - Internet-bound le trafic (`0.0.0.0/0`pour IPv4, `::/0` pour IPv6) est acheminé vers une passerelle Internet ()`igw-xxxxxxxxxx`. Cela signifie que le sous-réseau associé à la table de routage est un sous-réseau public.

> **Note**
>
> Si votre sous-réseau ne possède pas de bloc d'adresse CIDR IPv6, vous ne verrez que la route IPv4 (`0.0.0.0/0`).

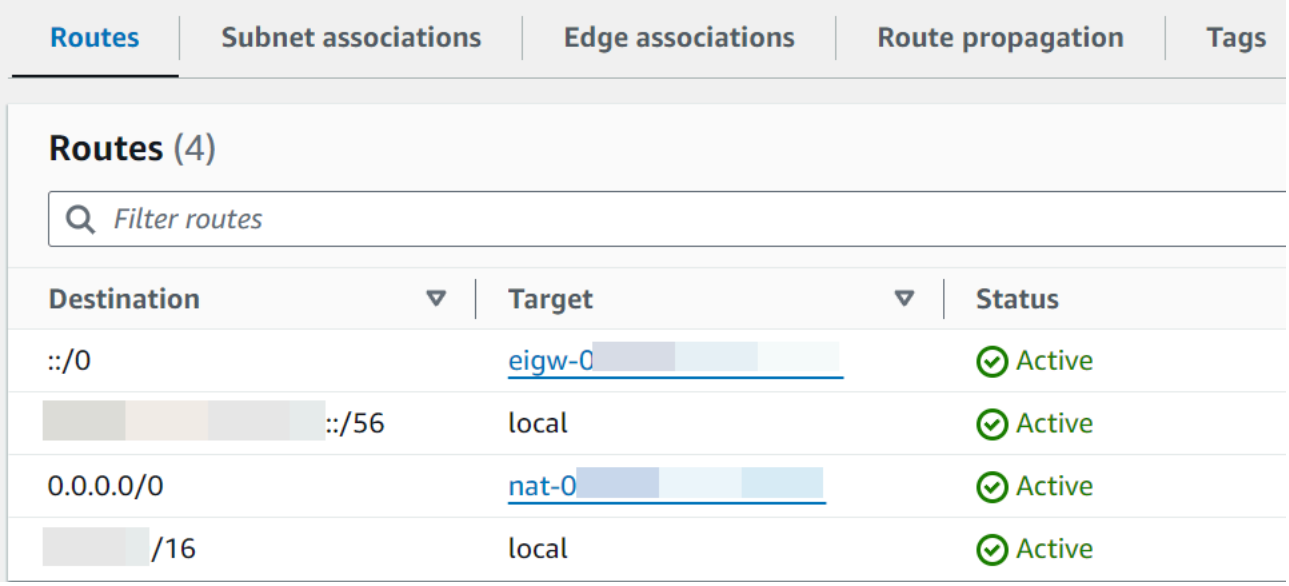
Example Table de routage de sous-réseau public



- Internet-bound le trafic pour IPv4 (`0.0.0.0/0`) est acheminé vers une passerelle NAT (`nat-xxxxxxxxxx`) associée à un sous-réseau public. Cela signifie que le sous-réseau est un sous-réseau privé qui peut accéder à l'Internet via la passerelle NAT.

> **Note**
>
> Si votre sous-réseau comporte un bloc CIDR IPv6, la table de routage doit également acheminer le trafic Internet IPv6 (`::/0`) vers une passerelle Internet de sortie uniquement (`eigw-xxxxxxxxxx`). Si votre sous-réseau ne possède pas de bloc d'adresse CIDR IPv6, vous ne verrez que la route IPv4 (`0.0.0.0/0`).

Example table de routage de sous-réseau privé



5. Répétez l'étape précédente jusqu'à ce que vous ayez examiné chaque table de routage associée à un sous-réseau de votre VPC et confirmé que vous disposez d'une table de routage avec une passerelle Internet et d'une table de routage avec une passerelle NAT.

   Si vous n'avez pas deux tables de routage, l'une avec une route vers une passerelle Internet et l'autre avec une route vers une passerelle NAT, suivez ces étapes pour créer les ressources manquantes et les entrées de table de routage.

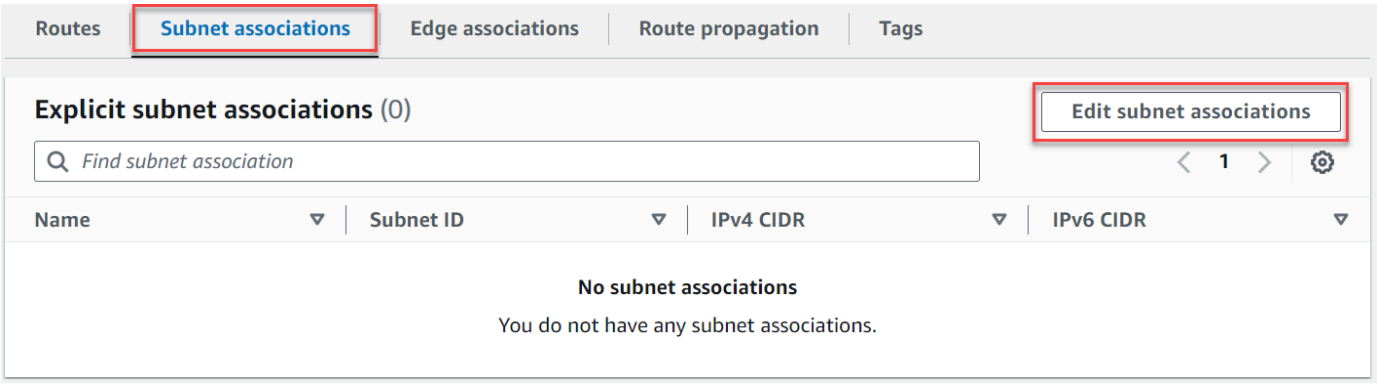
Création d'une table de routage

Suivez les étapes ci-dessous pour créer une table de routage et l'associer à un sous-réseau.

Pour créer une table de routage personnalisée à l'aide de la console Amazon VPC

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Route tables (Tables de routage).
3. Choisissez Créer une table de routage.
4. (Facultatif) Pour Nom, entrez un nom pour votre table de routage.
5. Pour VPC, choisissez votre VPC.
6. (Facultatif) Pour ajouter une identification, choisissez Add new tag (Ajouter une identification) et saisissez la clé et la valeur de l'identification.

7. Choisissez Créer une table de routage.
8. Sur l'onglet Associations de sous-réseau, choisissez Modifier les associations de sous-réseau.



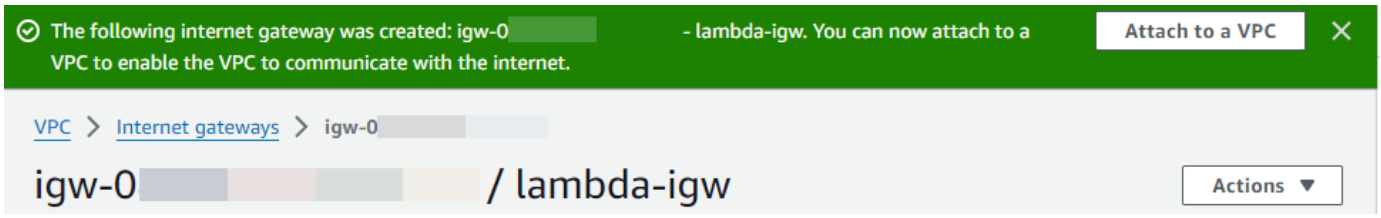
9. Sélectionnez la case à cocher pour le sous-réseau à associer à la table de routage.
10. Choisissez Save associations (Enregistrer les associations).

Création d'une passerelle Internet

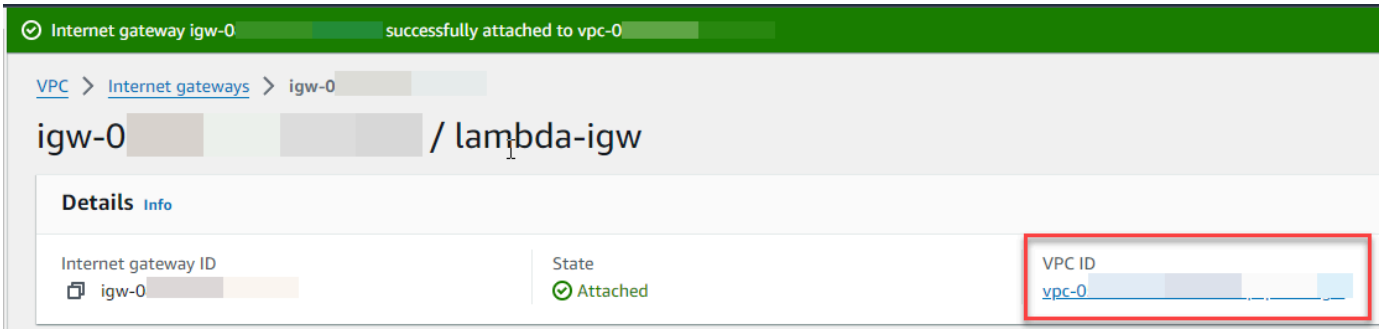
Procédez comme suit pour créer une passerelle Internet, l'associer à votre VPC et l'ajouter à la table de routage de votre sous-réseau public.

Pour créer une passerelle Internet

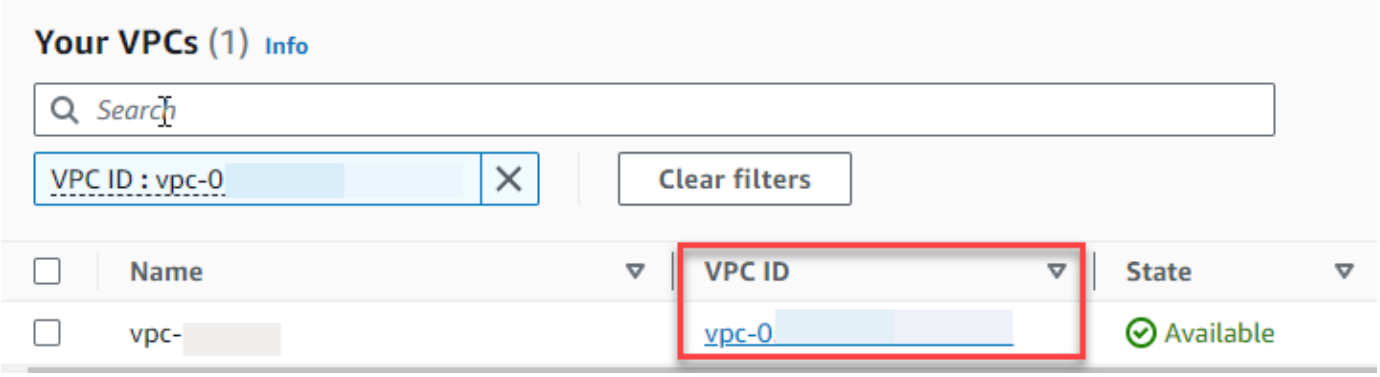
1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Passerelles Internet.
3. Choisissez Créer une passerelle Internet.
4. (Facultatif) Saisissez un nom pour votre passerelle Internet.
5. (Facultatif) Pour ajouter une identification, choisissez Add new tag (Ajouter une identification) et saisissez la clé et la valeur de l'identification.
6. Choisissez Créer une passerelle Internet.
7. Choisissez Attacher à un VPC dans la bannière en haut de l'écran, sélectionnez un VPC disponible, puis choisissez Attacher une passerelle Internet.



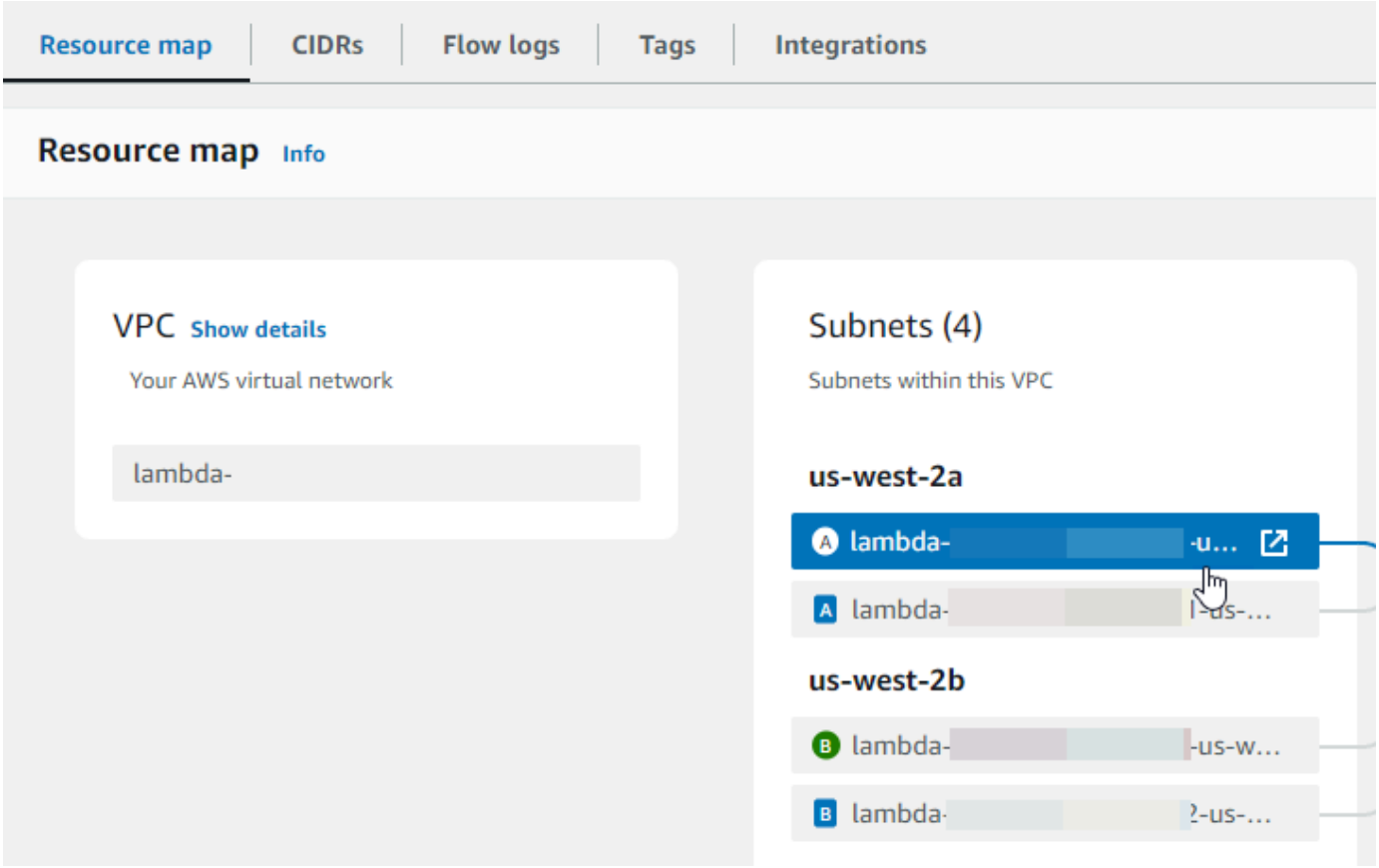
8. Choisissez l'ID de VPC.



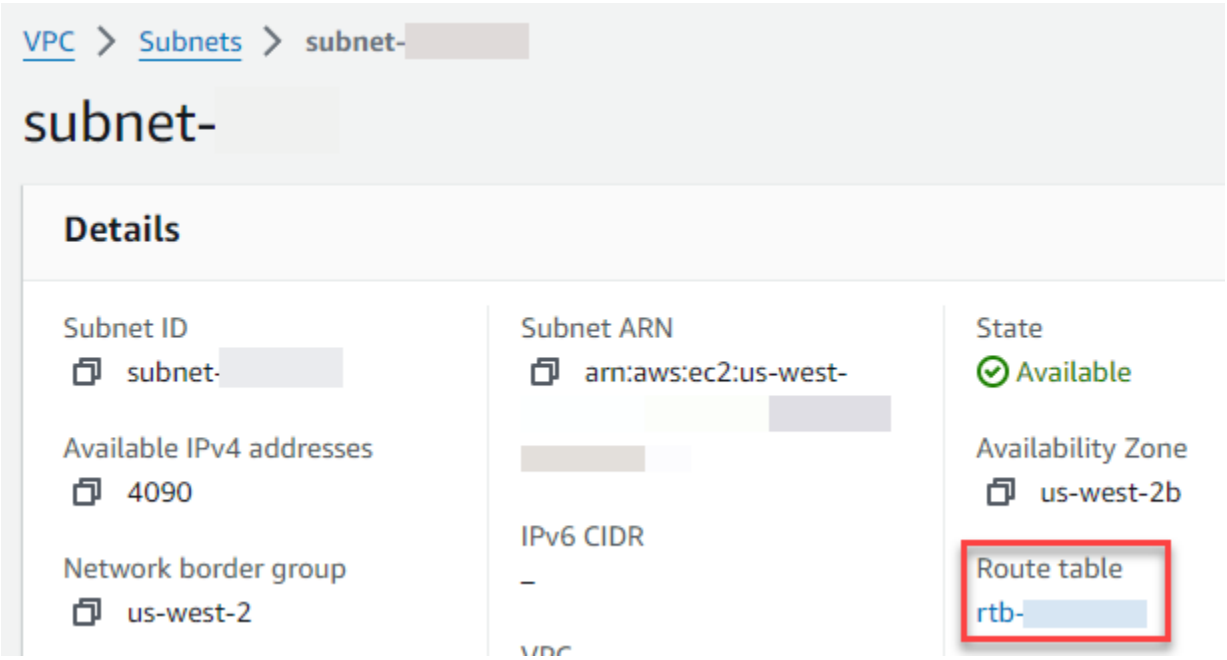
9. Sélectionnez à nouveau l'ID de VPC pour ouvrir la page des détails.



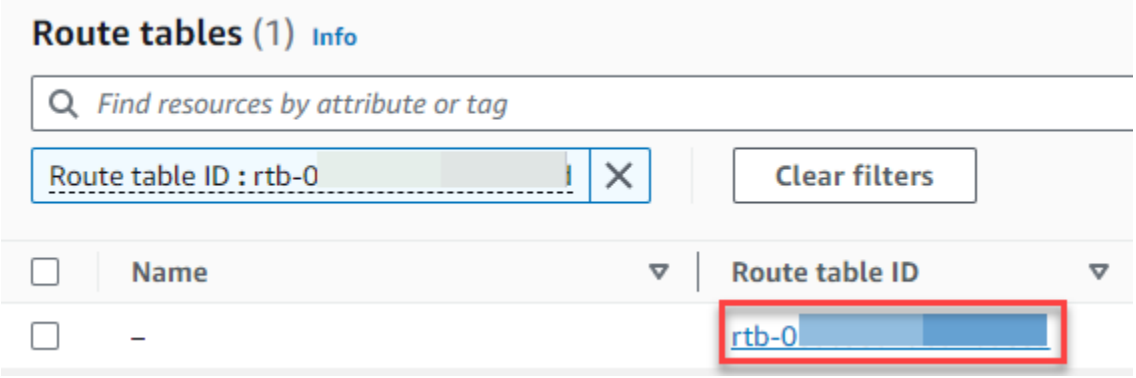
10. Faites défiler vers le bas jusqu'à la section Carte des ressources et choisissez un sous-réseau. Les détails du sous-réseau s'affichent dans un nouvel onglet.



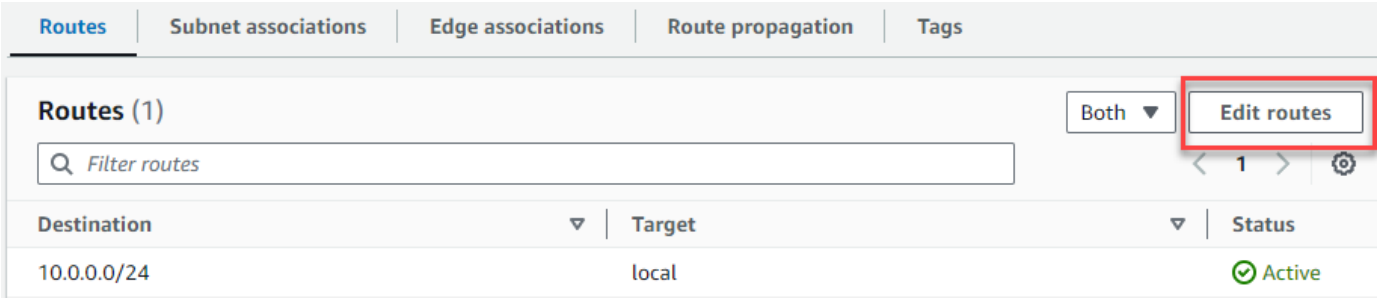
11. Cliquez sur le lien sous Table de routage.



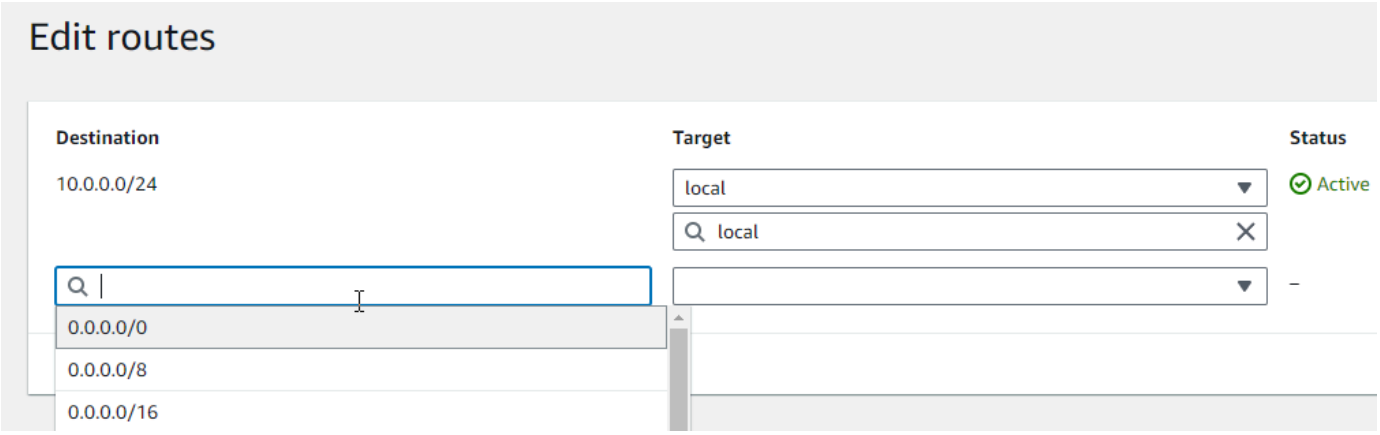
12. Choisissez l'ID de la table de routage pour ouvrir la page de détails de la table de routage.



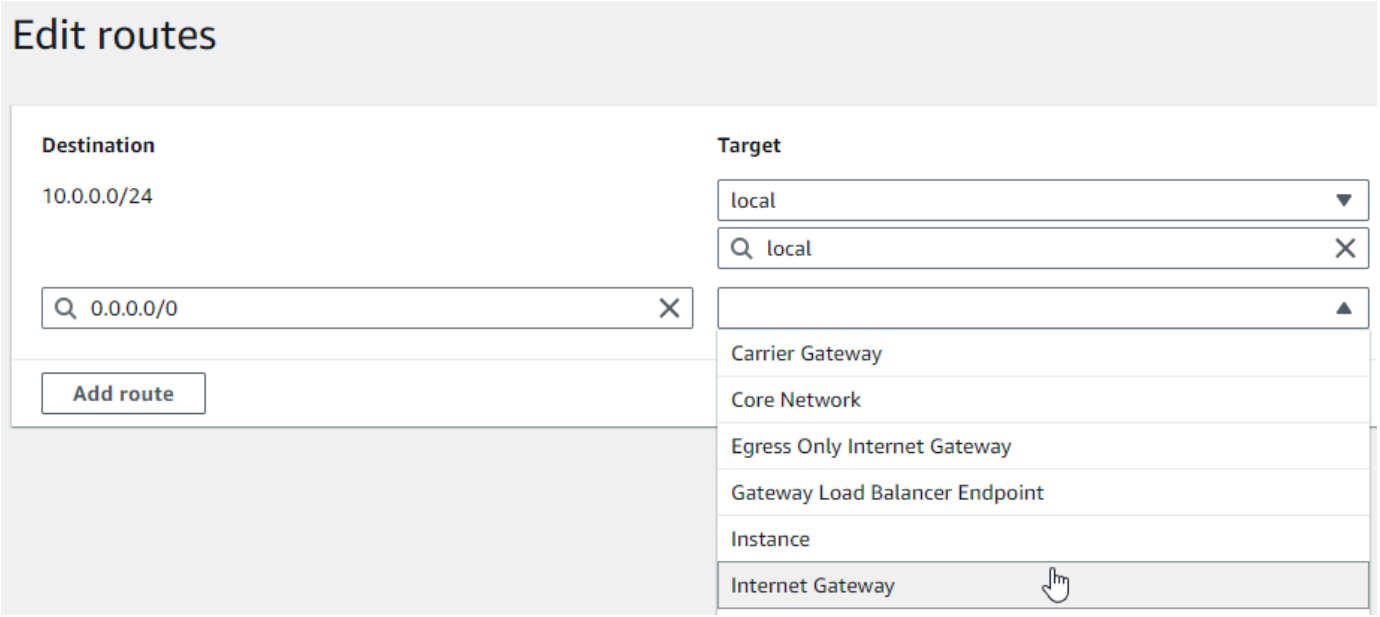
13. Sous Routes, choisissez la Modifier des routes.



14. Choisissez Ajouter une route, puis saisissez `0.0.0.0/0` dans la zone Destination.



15. Pour Cible, sélectionnez Passerelle Internet, puis choisissez la passerelle Internet que vous avez créée précédemment. Si votre sous-réseau comporte un bloc CIDR IPv6, vous devez également ajouter une route pour `::/0` vers la même passerelle Internet.



16. Cliquez sur Enregistrer les modifications.

Créer une passerelle NAT

Suivez ces étapes pour créer une passerelle NAT, l'associer à un sous-réseau public, puis l'ajouter à la table de routage de votre sous-réseau privé.

Pour créer une passerelle NAT et l'associer à un sous-réseau public

1. Dans le volet de navigation, sélectionnez Passerelles NAT.
2. Sélectionnez Créer une passerelle NAT.
3. (Facultatif) Saisissez un nom pour votre passerelle NAT.
4. Pour Sous-réseau, sélectionnez le sous-réseau public dans votre VPC. (Un sous-réseau public est un sous-réseau qui a une entrée de table de routage comportant une route vers une passerelle Internet)

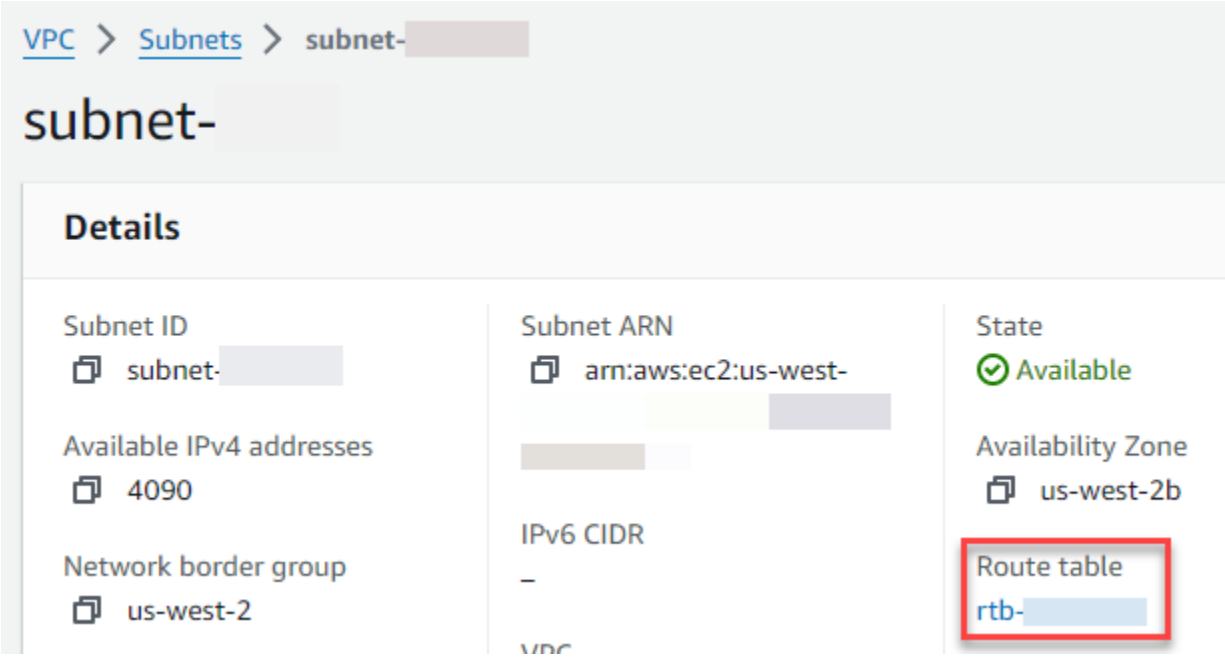
> **Note**
>
> Les passerelles NAT sont associées à un sous-réseau public, mais l'entrée de la table de routage se trouve dans le sous-réseau privé.

5. Pour ID d'allocation IP élastique, sélectionnez une adresse IP élastique ou choisissez Allouer une adresse IP élastique.

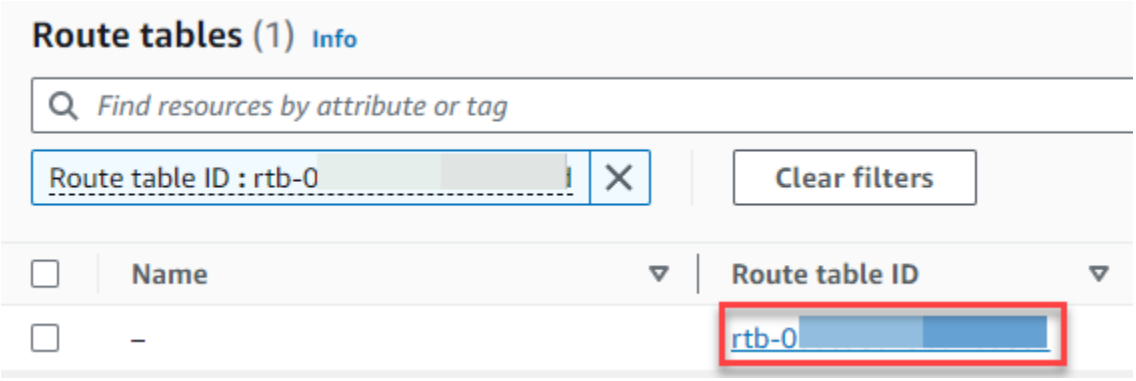
6. Sélectionnez Créer une passerelle NAT.

Pour ajouter une route vers la passerelle NAT dans la table de routage du sous-réseau privé

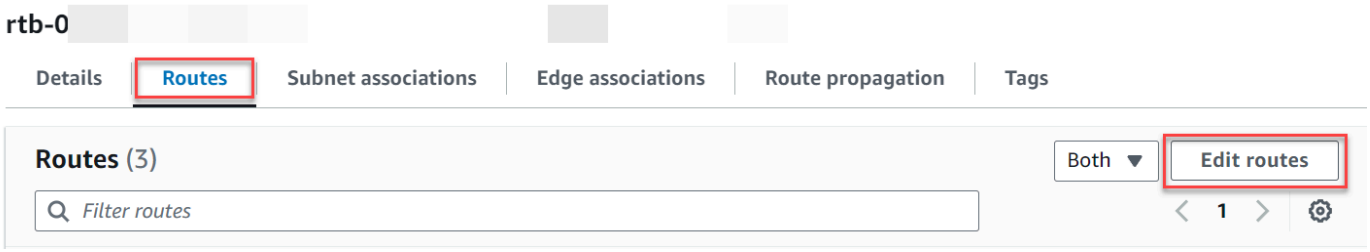
1. Dans le panneau de navigation, choisissez Subnets (Sous-réseaux).
2. Sélectionnez un sous-réseau privé dans votre VPC. (Un sous-réseau privé est un sous-réseau qui ne comporte pas de route vers une passerelle Internet dans sa table de routage)
3. Cliquez sur le lien sous Table de routage.



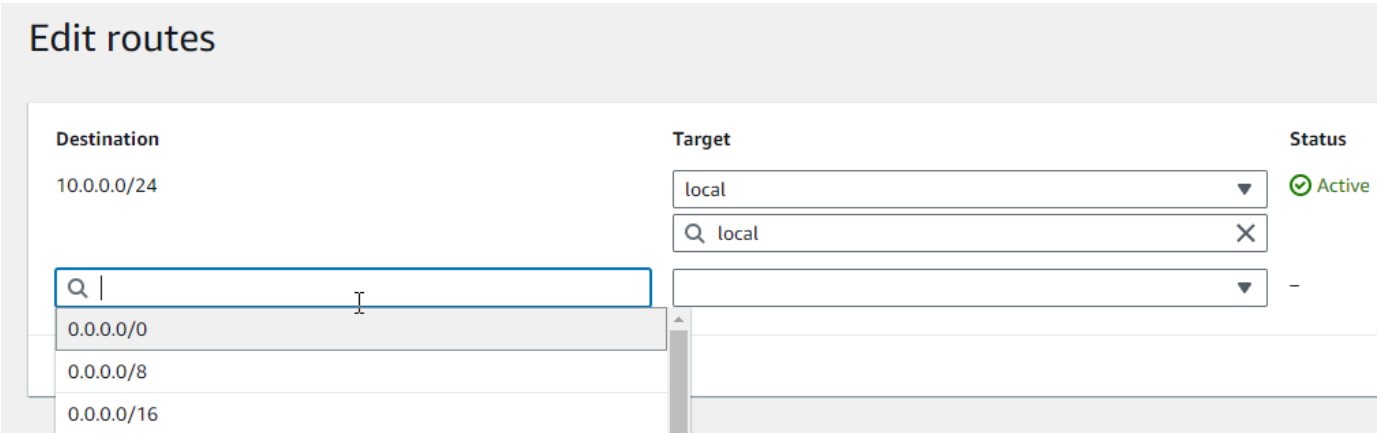
4. Choisissez l'ID de la table de routage pour ouvrir la page de détails de la table de routage.



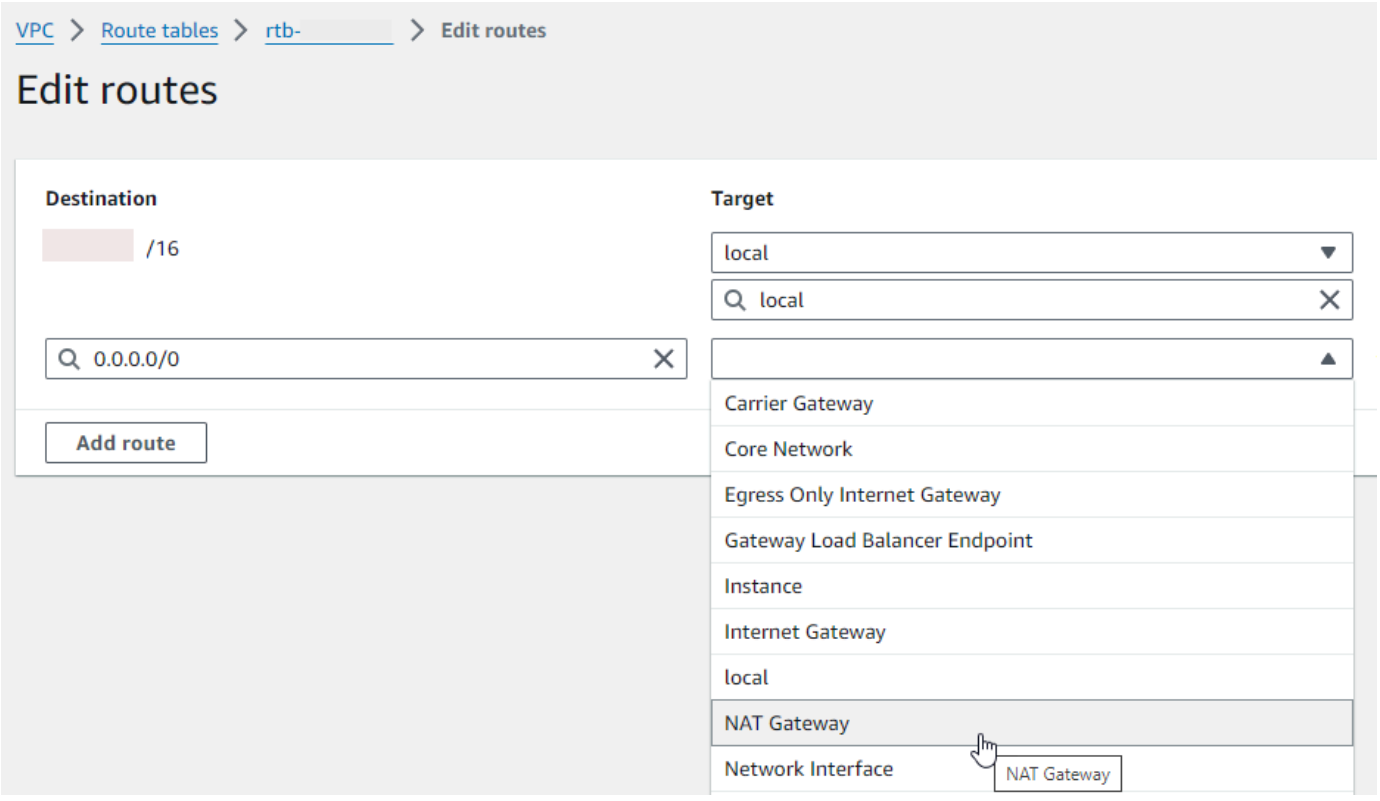
5. Choisissez l'onglet Routes, puis Modifier des routes.



6. Choisissez Ajouter une route, puis saisissez `0.0.0.0/0` dans la zone Destination.



7. Pour Cible, choisissez Passerelle NAT, puis sélectionnez la passerelle NAT que vous avez créée.



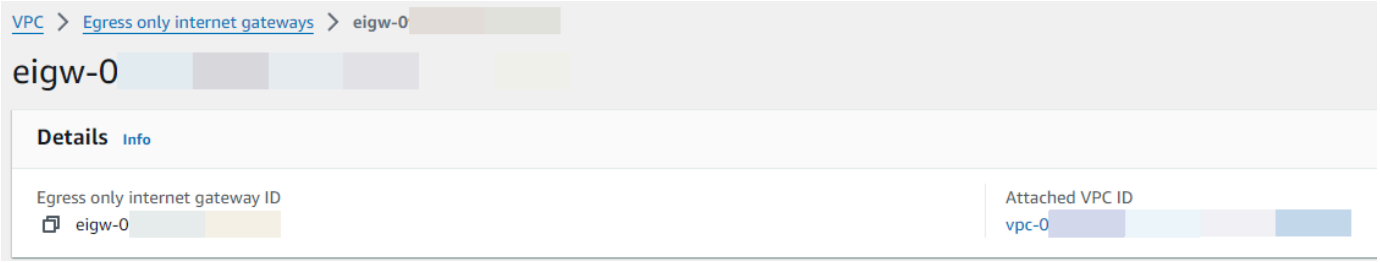
8. Cliquez sur Enregistrer les modifications.

Création d'une passerelle Internet de sortie uniquement (limité à IPv6)

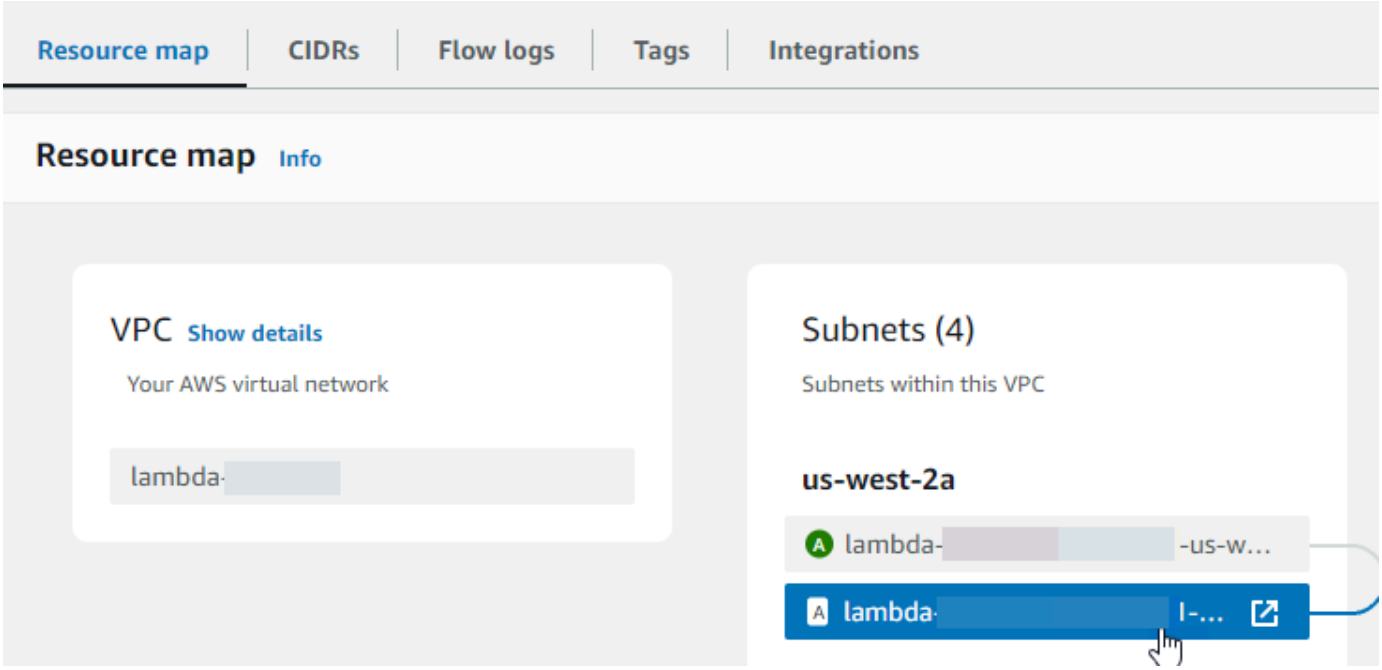
Procédez comme suit pour créer une passerelle Internet de sortie uniquement et l'ajouter à la table de routage de votre sous-réseau privé.

Pour créer une passerelle Internet de sortie uniquement

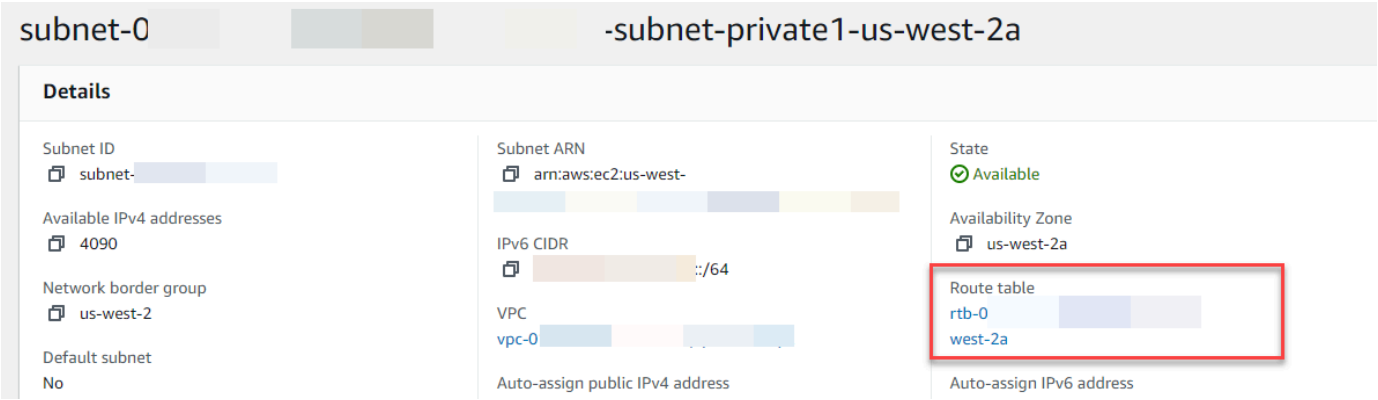
1. Dans le volet de navigation, choisissez les passerelles Egress-only Internet.
2. Choisissez Créer une passerelle Internet de sortie uniquement.
3. (Facultatif) Saisissez un nom.
4. Sélectionnez le VPC dans lequel créer la passerelle Internet de sortie uniquement.
5. Choisissez Créer une passerelle Internet de sortie uniquement.
6. Choisissez le lien sous ID du VPC attaché.



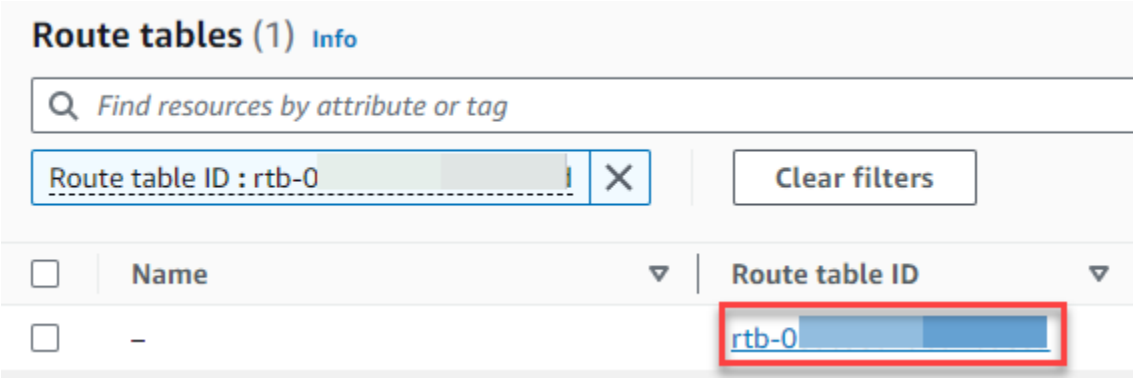
7. Sélectionnez le lien sous l'ID de VPC pour ouvrir la page des détails.
8. Faites défiler vers le bas jusqu'à la section Carte des ressources et choisissez un sous-réseau privé. (Un sous-réseau privé est un sous-réseau qui ne comporte pas de route vers une passerelle Internet dans sa table de routage) Les détails du sous-réseau s'affichent dans un nouvel onglet.



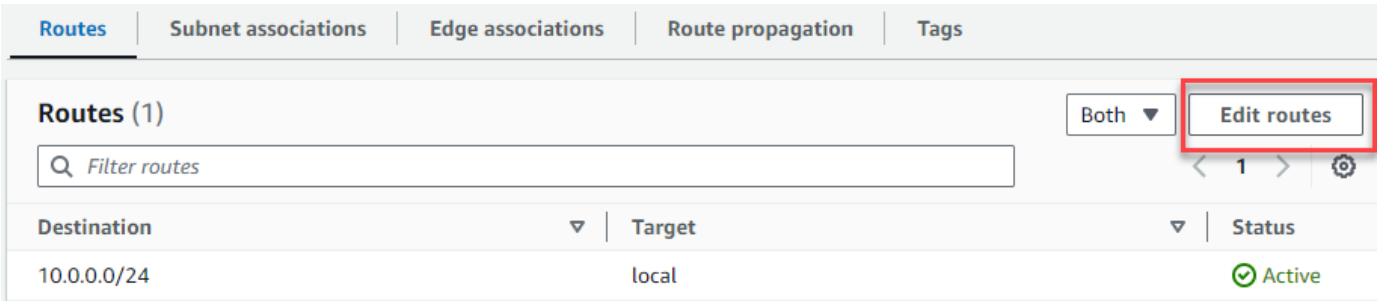
9. Cliquez sur le lien sous Table de routage.



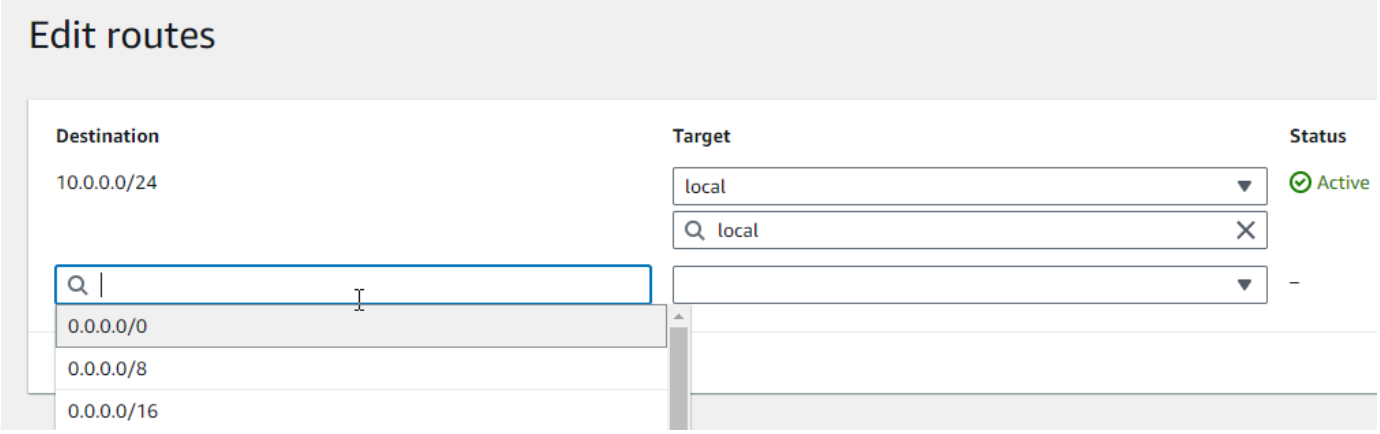
10. Choisissez l'ID de la table de routage pour ouvrir la page de détails de la table de routage.



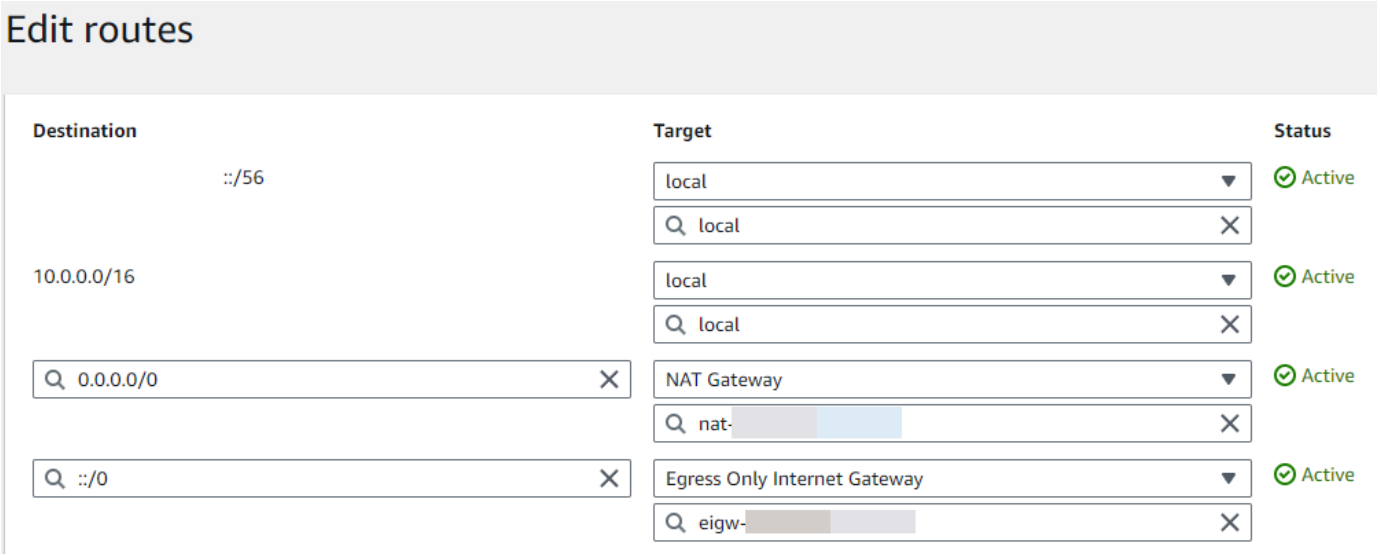
11. Sous Routes, choisissez la Modifier des routes.



12. Choisissez Ajouter une route, puis saisissez `::/0` dans la zone Destination.



13. Pour Cible, sélectionnez Passerelle Internet de sortie uniquement, puis choisissez la passerelle que vous avez créée précédemment.



14. Cliquez sur Enregistrer les modifications.

Configurer la fonction Lambda

Pour configurer un VPC lorsque vous créez une fonction

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez Create Event Function.
3. Sous Informations de base, dans Nom de fonction, entrez un nom pour votre fonction.
4. Développez Advanced settings (Paramètres avancés).
5. Sélectionnez Activer le VPC, puis choisissez un VPC.
6. (Facultatif) Pour autoriser le trafic IPv6 sortant, sélectionnez Autoriser le trafic IPv6 pour les sous-réseaux à double pile.
7. Pour Sous-réseaux, sélectionnez tous les sous-réseaux privés. Les sous-réseaux privés peuvent accéder à Internet via une passerelle NAT. La connexion d'une fonction à un sous-réseau public ne lui donne pas accès à Internet.

   > **Note**
   >
   > Si vous avez sélectionné Autoriser le trafic IPv6 pour les sous-réseaux à double pile, tous les sous-réseaux sélectionnés doivent avoir un bloc CIDR IPv4 et un bloc CIDR IPv6.

8. Pour les groupes de sécurité, sélectionnez un groupe de sécurité qui autorise le trafic sortant.
9. Choisissez Create Event Function.

Lambda crée automatiquement un rôle d'exécution avec la politique AWSLambdaVPCAccessExecutionRole AWS gérée. Les autorisations de cette politique ne sont nécessaires que pour créer des interfaces réseau élastiques pour la configuration VPC, et non pour invoquer votre fonction. Pour appliquer les autorisations de moindre privilège, vous pouvez supprimer la AWSLambdaVPCAccessExecutionRolepolitique de votre rôle d'exécution après avoir créé la fonction et la configuration VPC. Pour plus d'informations, consultez Autorisations IAM requises.

Pour configurer un VPC pour une fonction existante

Pour ajouter une configuration VPC à une fonction existante, le rôle d'exécution de la fonction doit être autorisé à créer et à gérer des interfaces réseau élastiques. La politique AWSLambdaVPCAccessExecutionRole AWS gérée inclut les autorisations requises. Pour appliquer les autorisations de moindre privilège, vous pouvez supprimer la

AWSLambdaVPCAccessExecutionRolepolitique de votre rôle d'exécution après avoir créé la configuration VPC.

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez une fonction.
3. Choisissez l'onglet Configuration puis choisissez VPC.
4. Sous VPC, choisissez Modifier.
5. Sélectionnez le VPC.
6. (Facultatif) Pour autoriser le trafic IPv6 sortant, sélectionnez Autoriser le trafic IPv6 pour les sous-réseaux à double pile.
7. Pour Sous-réseaux, sélectionnez tous les sous-réseaux privés. Les sous-réseaux privés peuvent accéder à Internet via une passerelle NAT. La connexion d'une fonction à un sous-réseau public ne lui donne pas accès à Internet.

   > **Note**
   >
   > Si vous avez sélectionné Autoriser le trafic IPv6 pour les sous-réseaux à double pile, tous les sous-réseaux sélectionnés doivent avoir un bloc CIDR IPv4 et un bloc CIDR IPv6.

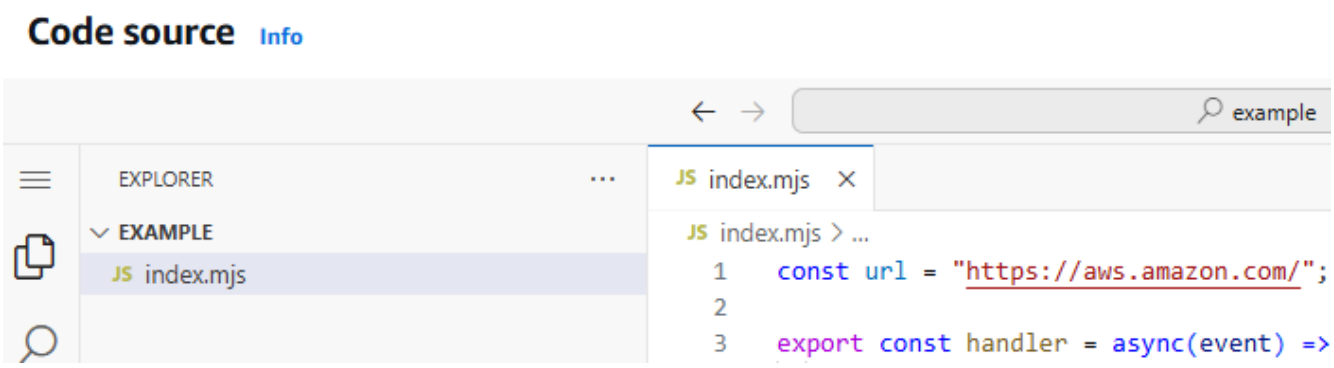
8. Pour les groupes de sécurité, sélectionnez un groupe de sécurité qui autorise le trafic sortant.
9. Cliquez sur Enregistrer.

Tester la fonction

Utilisez l'exemple de code suivant pour vérifier que votre VPC-connected fonction peut accéder à l'Internet public. En cas de succès, le code renvoie un code d'état `200`. En cas d'échec, la fonction expire.

Node.js

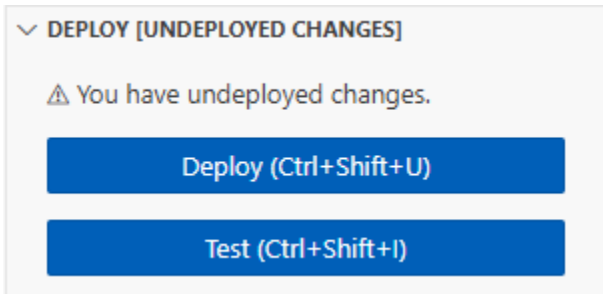
1. Dans le volet Source du code de la console Lambda, collez le code suivant dans le fichier index.mjs. La fonction envoie une requête HTTP GET à un point de terminaison public et renvoie le code de réponse HTTP pour tester si la fonction a accès à l'Internet public.



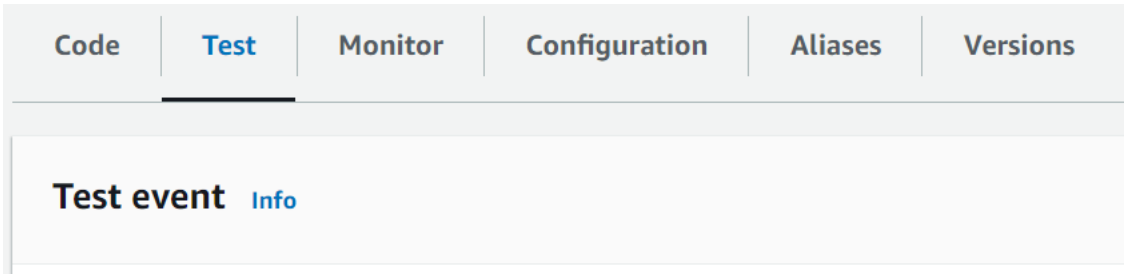
Example— Requête HTTP avec async/await

```
const url = "https://aws.amazon.com/";

export const handler = async(event) => {
    try {
        const res = await fetch(url);
        console.info("status", res.status);
        return res.status;
    }
    catch (e) {
        console.error(e);
        return 500;
    }
};
```

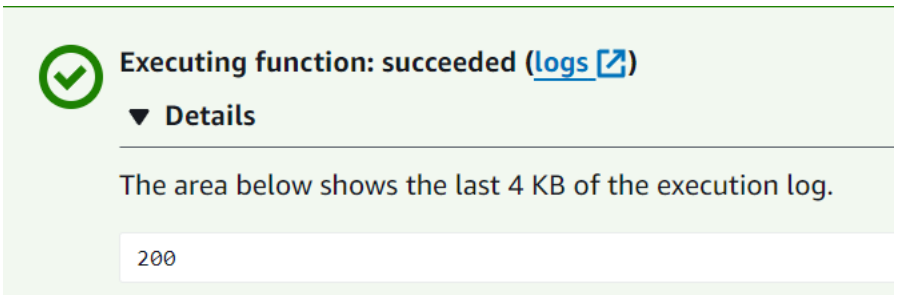
2. Dans la section DÉPLOYER, choisissez Déployer pour mettre à jour le code de votre fonction :



3. Choisissez l'onglet Test.



4. Sélectionnez Tester).
5. La fonction renvoie un code d'état `200`. Cela signifie que la fonction dispose d'un accès Internet sortant.

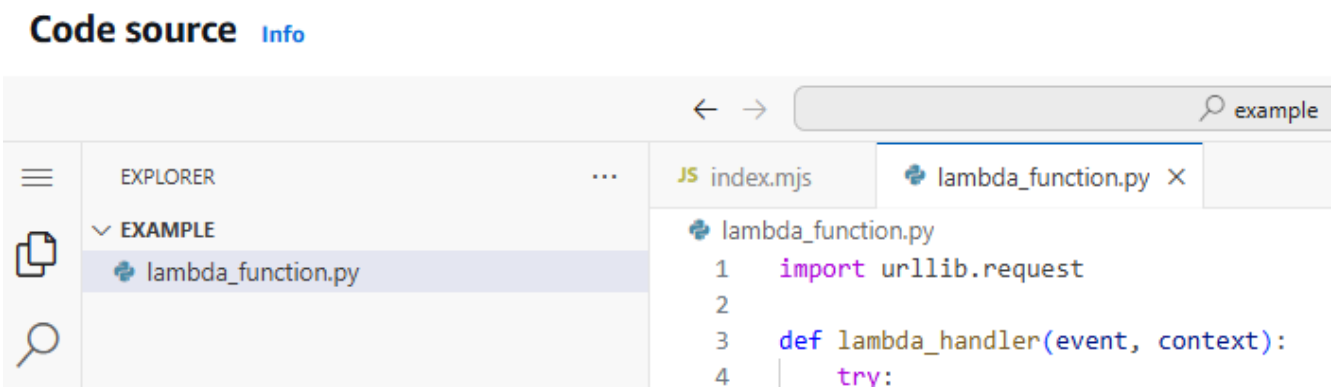


Si la fonction ne parvient pas à accéder à l'Internet public, un message d'erreur de ce type s'affiche :

```
{
  "errorMessage": "2024-04-11T17:22:20.857Z abe12jlc-640a-8157-0249-9be825c2y110
 Task timed out after 3.01 seconds"
}
```

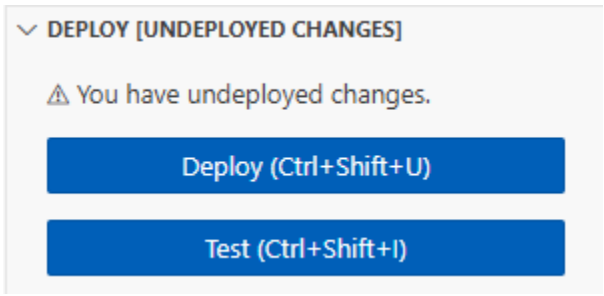
Python

1. Dans le volet Source du code de la console Lambda, collez le code suivant dans le fichier lambda_function.py. La fonction envoie une requête HTTP GET à un point de terminaison public et renvoie le code de réponse HTTP pour tester si la fonction a accès à l'Internet public.

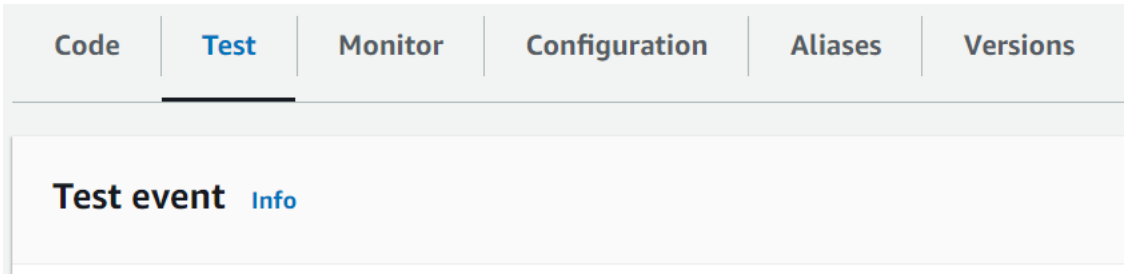



```
import urllib.request

def lambda_handler(event, context):
    try:
        response = urllib.request.urlopen('https://aws.amazon.com')
        status_code = response.getcode()
        print('Response Code:', status_code)
        return status_code
    except Exception as e:
        print('Error:', e)
        raise e
```

2. Dans la section DÉPLOYER, choisissez Déployer pour mettre à jour le code de votre fonction :

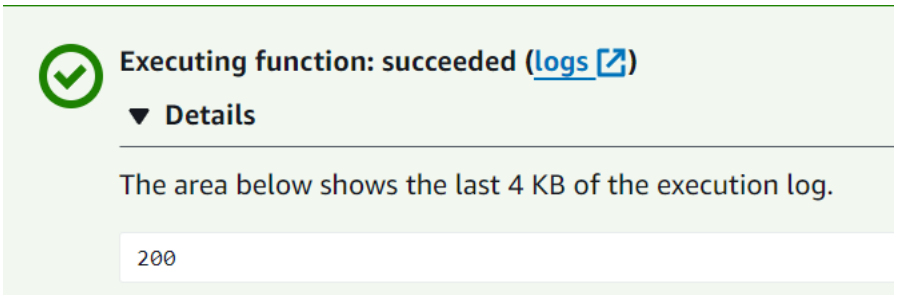


3. Choisissez l'onglet Test.



4. Sélectionnez Tester).

5. La fonction renvoie un code d'état `200`. Cela signifie que la fonction dispose d'un accès Internet sortant.



Si la fonction ne parvient pas à accéder à l'Internet public, un message d'erreur de ce type s'affiche :

```
{
  "errorMessage": "2024-04-11T17:22:20.857Z abe12jlc-640a-8157-0249-9be825c2y110
 Task timed out after 3.01 seconds"
}
```

Connexion des points de terminaison d'un VPC de l'interface entrante pour Lambda

Si vous utilisez Amazon Virtual Private Cloud (Amazon VPC) pour héberger vos AWS ressources, vous pouvez établir une connexion entre votre VPC et Lambda. Vous pouvez utiliser cette connexion pour invoquer votre fonction Lambda sans traverser l'Internet public.

Pour établir une connexion privée entre votre VPC et Lambda, créez un point de terminaison de VPC d'interface. Les points de terminaison d'interface sont alimentés par AWS PrivateLink. Avec AWS PrivateLink, vous pouvez accéder en privé aux API Lambda sans passerelle Internet, périphérique NAT, connexion VPN ou AWS Direct Connect connexion. Les instances dans votre VPC n'ont pas besoin d'adresses IP publiques pour communiquer avec des API Lambda. Le trafic entre votre VPC et Lambda ne quitte pas le réseau AWS .

Chaque point de terminaison d'interface est représenté par une ou plusieurs interfaces réseau Elastic dans vos sous-réseaux. Une interface réseau fournit une adresse IP privée qui sert de point d'entrée au trafic vers Lambda.

Sections

- Considérations relatives aux points de terminaison d'interface Lambda
- Création d'un point de terminaison d'interface pour Lambda
- Création d'une stratégie de point de terminaison d'interface pour Lambda

Considérations relatives aux points de terminaison d'interface Lambda

Avant de configurer un point de terminaison d'interface pour Lambda, consulter Propriétés et limites des points de terminaison d'interface dans le Guide de l'utilisateur Amazon VPC.

Vous pouvez appeler n'importe quelle opération d'API Lambda à partir de votre VPC. Par exemple, vous pouvez invoquer la fonction Lambda en appelant l'API `Invoke` à partir de votre VPC. Pour obtenir la liste complète des API Lambda, consultez Actions dans la Référence API Lambda.

`use1-az3` est une région à capacité limitée pour les fonctions Lambda VPC. Vous ne devez pas utiliser de sous-réseaux dans cette zone de disponibilité avec vos fonctions Lambda, car cela peut réduire la redondance zonale en cas de panne.

Keep-alive pour les connexions persistantes

Lambda purgeant les connexions inactives au fil du temps, vous devez utiliser une directive keep-alive pour maintenir les connexions persistantes. Si vous tentez de réutiliser une connexion inactive lorsque vous invoquez une fonction, cela entraîne une erreur de connexion. Pour maintenir votre connexion persistante, utilisez la directive Keep-alive associée à votre environnement d'exécution. Pour un exemple, consultez la section Réutiliser les connexions avec Keep-Alive in Node.js dans le Guide du AWS SDK pour JavaScript développeur.

Considérations sur la facturation

L'accès à une fonction Lambda via un point de terminaison d'interface n'occasionne aucun coût supplémentaire. Pour plus d'informations sur la tarification de Lambda, consultez Tarification AWS Lambda.

La tarification standard AWS PrivateLink s'applique aux points de terminaison de l'interface pour Lambda. Votre AWS compte est facturé pour chaque heure pendant laquelle un point de terminaison d'interface est provisionné dans chaque zone de disponibilité et pour les données traitées via le point de terminaison de l'interface. Pour plus d'informations sur la tarification des points de terminaison d'interface, consultez Tarification AWS PrivateLink.

Considérations sur l'appairage de VPC

Vous pouvez connecter d'autres VPC au VPC avec des points de terminaison d'interface à l'aide d'un Appairage de VPC. L'appairage de VPC est une connexion réseau entre deux VPC. Vous pouvez aussi établir une connexion d'appairage de VPC entre vos deux VPC, ou avec un VPC situé dans un autre compte AWS . Les VPC peuvent également se trouver dans deux AWS régions différentes.

Le trafic entre les VPC homologues reste sur le AWS réseau et ne passe pas par l'Internet public. Une fois les VPC connectés, les ressources telles que les instances Amazon Elastic Compute Cloud (Amazon EC2), les instances Amazon Relational Database Service (Amazon RDS) ou les fonctions VPC-enabled Lambda des deux VPC peuvent accéder à l'API Lambda via des points de terminaison d'interface créés dans l'un des VPC.

Création d'un point de terminaison d'interface pour Lambda

Vous pouvez créer un point de terminaison d'interface pour Lambda à l'aide de la console Amazon VPC ou du AWS Command Line Interface ()AWS CLI. Pour de plus amples informations, veuillez consulter Création d'un point de terminaison d'interface dans le Amazon VPC Guide de l'utilisateur.

Pour créer un point de terminaison d'interface pour Lambda (console)

1. Ouvrez la page Points de terminaison de la console Amazon VPC.
2. Choisissez Créer un point de terminaison.
3. Pour Catégorie de service, assurez-vous que Services AWS est sélectionné.
4. Dans le champ Nom du service, choisissez com.amazonaws. ***region***.lambda. Vérifiez que le Type est Interface.
5. Choisissez un VPC et des sous-réseaux
6. Pour activer un DNS privé pour le point de terminaison d'interface, sélectionnez la case à cocher Enable DNS Name (Activer le nom de DNS). Nous vous recommandons d'activer des noms d'hôtes DNS privés pour votre point de terminaison de VPC pour les Services AWS. Cela garantit que les demandes qui utilisent les points de terminaison du service public, telles que les demandes effectuées via un AWS SDK, sont résolues vers votre point de terminaison VPC.
7. Pour Groupes de sécurité, choisissez un ou plusieurs groupes de sécurité.
8. Choisissez Créer un point de terminaison.

Pour utiliser l'option de DNS privée, vous devez définir les `enableDnsHostnames` et `enableDnsSupportattributes` de votre VPC. Pour plus d'informations, consultez Affichage et mise à jour de la prise en charge de DNS pour votre VPC dans le Guide de l'utilisateur Amazon VPC. Si vous activez le DNS privé pour le point de terminaison d'interface, vous pouvez adresser des demandes d'API à Lambda en utilisant son nom DNS par défaut pour la région, par exemple, `lambda.us-east-1.amazonaws.com`. Pour plus de points de terminaison de service, consultez Points de terminaison de service et quotas dans le Références générales AWS.

Pour plus d'informations, consultez Accès à un service via un point de terminaison d'interface dans le Guide de l'utilisateur Amazon VPC.

Pour plus d'informations sur la création et la configuration d'un point de terminaison à l'aide de CloudFormation, consultez la ressource AWS : :EC2 : :VPCENdpoint dans le Guide de l'utilisateur. AWS CloudFormation

Pour créer un point de terminaison d'interface pour Lambda (AWS CLI)

Utilisez la commande create-vpc-endpoint et spécifiez l'ID du VPC, le type de point de terminaison du VPC (interface), le nom du service, les sous-réseaux qui utilisent le point de terminaison et les groupes de sécurité à associer aux interfaces réseau du point de terminaison. Par exemple :

```
aws ec2 create-vpc-endpoint
  --vpc-id vpc-ec43eb89
  --vpc-endpoint-type Interface
  --service-name com.amazonaws.us-east-1.lambda
  --subnet-id subnet-abababab
  --security-group-id sg-1a2b3c4d
```

Création d'une stratégie de point de terminaison d'interface pour Lambda

Pour contrôler qui peut utiliser votre point de terminaison d'interface, ainsi que les fonctions Lambda auxquelles l'utilisateur peut accéder, vous pouvez attacher une stratégie de point de terminaison à votre point de terminaison. La stratégie spécifie les informations suivantes :

- Le principal qui peut exécuter des actions.
- Les actions que le principal peut effectuer.
- Ressources sur lesquelles le principal peut effectuer des actions.

Pour de plus amples informations, veuillez consulter Contrôle de l'accès aux services avec points de terminaison d'un VPC dans le Amazon VPC Guide de l'utilisateur.

Exemple : stratégie de point de terminaison d'interface pour des actions Lambda

Voici un exemple de stratégie de point de terminaison pour Lambda. Lorsqu'elle est attachée à un point de terminaison, cette stratégie permet à l'utilisateur `MyUser` d'invoquer la fonction `my-function`.

> **Note**
>
> Vous devez inclure les ARN de la fonction qualifiée et de celle non qualifiée dans la ressource.

```
{
   "Statement":[
      {
         "Principal":
         {
             "AWS": "arn:aws:iam::111122223333:user/MyUser"
         },
```

```
         "Effect":"Allow",
         "Action":[
            "lambda:InvokeFunction"
         ],
         "Resource": [
               "arn:aws:lambda:us-east-2:123456789012:function:my-function",
               "arn:aws:lambda:us-east-2:123456789012:function:my-function:*"
            ]
      }
   ]
}
```

Pour permettre à votre fonction d'accéder aux ressources d'un VPC appartenant à un autre Compte AWS, consultezthe section called “Attachement de fonctions aux ressources d’un autre compte”.

Configuration de l'accès au système de fichiers pour les fonctions d'événement Lambda

Vous pouvez configurer une fonction Lambda pour monter un système de fichiers dans un répertoire local. Lambda prend en charge les types de systèmes de fichiers suivants :

- Amazon Elastic File System (Amazon EFS) : système de fichiers sans serveur qui s'adapte automatiquement à vos charges de travail.
- Amazon S3 Files : système de fichiers sans serveur pour le montage de votre compartiment Amazon S3. Amazon S3 Files permet d'accéder à vos objets Amazon S3 sous forme de fichiers à l'aide d'opérations de système de fichiers standard telles que la lecture et l'écriture sur le chemin de montage local.

> **Note**
>
> Une fonction Lambda peut utiliser Amazon EFS ou Amazon S3 Files, mais pas les deux. Si votre fonction est déjà configurée avec un type de système de fichiers, vous devez le supprimer avant de configurer l'autre.

Configuration de l'accès au système de fichiers Amazon EFS

Vous pouvez configurer une fonction pour monter un système de fichiers Amazon Elastic File System (Amazon EFS) dans un répertoire local. Amazon EFS est un système de fichiers sans serveur qui s'adapte automatiquement à vos charges de travail. Avec Amazon EFS, votre code de fonction peut accéder aux ressources partagées et les modifier en toute sécurité et avec une haute simultanéité.

Sections

- Rôle d'exécution et autorisations utilisateur
- Configuration d'un système de fichiers et d'un point d'accès
- Connexion à un système de fichiers (console)
- Régions prises en charge

Rôle d'exécution et autorisations utilisateur

Si le système de fichiers n'a pas de stratégie configurée par l'utilisateur Gestion des identités et des accès AWS (IAM), EFS utilise une politique par défaut qui accorde un accès complet à tout client qui peut se connecter au système de fichiers à l'aide d'une cible de montage du système de fichiers. Si le système de fichiers dispose d'une stratégie IAM configurée par l'utilisateur, le rôle d'exécution de votre fonction doit avoir le bon.`elasticfilesystem`Autorisations.

Autorisations du rôle d’exécution

- système de fichiers élastique : ClientMount
- elasticfilesystem : ClientWrite (non requis pour les connexions en lecture seule)

Ces autorisations sont incluses dans la politique AmazonElasticFileSystemClientReadWriteAccessgérée. En outre, votre rôle d'exécution doit posséder leautorisations requises pour se connecter au VPC du système de fichiers.

Lorsque vous configurez un système de fichiers, Lambda utilise vos autorisations pour vérifier les cibles de montage. Pour configurer une fonction pour vous connecter à un système de fichiers, votre utilisateur a besoin des autorisations suivantes :

Autorisations des utilisateurs

- système de fichiers élastique : DescribeMountTargets

Configuration d'un système de fichiers et d'un point d'accès

Créez un système de fichiers Amazon EFS avec une cible de montage dans chaque zone de disponibilité à laquelle votre fonction se connecte. Pour les performances et une résilience, utilisez au moins deux zones de disponibilité. Par exemple, dans une configuration simple, vous pouvez avoir un VPC avec deux sous-réseaux privés dans des zones de disponibilité distinctes. La fonction se connecte aux deux sous-réseaux et une cible de montage est disponible dans chacun. Assurez-vous que le trafic NFS (port 2049) est autorisé par les groupes de sécurité utilisés par la fonction et les cibles de montage.

> **Note**
>
> Lorsque vous créez un système de fichiers, vous choisissez un mode de performances qui ne peut pas être modifié ultérieurement. Le mode à usage général a une latence plus faible,

tandis que le I/O mode Max prend en charge un débit maximal et des IOPS plus élevés. Pour orienter votre choix, consultez Performances d'Amazon EFS dans le Guide de l'utilisateur Amazon Elastic File System.

Un point d'accès relie chaque instance de la fonction à la cible de montage droite pour la zone de disponibilité à laquelle elle se connecte. Pour des performances optimales, créez un point d'accès avec un chemin non racine et limitez le nombre de fichiers que vous créez dans chaque répertoire. L'exemple suivant crée un répertoire nommé `my-function` sur le système de fichiers et définit l'ID propriétaire sur 1001 avec les autorisations d'annuaire standard (755).

Example configuration du point d'accès

- Nom – `files`
- ID de l'utilisateur – `1001`
- ID du groupe – `1001`
- Chemin – `/my-function`
- Permissions (Autorisations – `755`
- ID d'utilisateur du propriétaire – `1001`
- ID d'utilisateur du groupe – `1001`

Lorsqu'une fonction utilise le point d'accès, elle reçoit l'ID utilisateur 1001 et dispose d'un accès complet au répertoire.

Pour plus d'informations, consultez les rubriques suivantes dans le Guide de l'utilisateur Amazon Elastic File System User.

- Création de ressources pour Amazon EFS
- Collaboration avec des utilisateurs, des groupes et des autorisations

Connexion à un système de fichiers (console)

Une fonction se connecte à un système de fichiers sur le réseau local dans un VPC. Les sous-réseaux auquel votre fonction se connecte peuvent être les mêmes sous-réseaux qui contiennent des points de montage pour votre système de fichiers, ou des sous-réseaux de la même zone de disponibilité qui peuvent acheminer le trafic NFS (port 2049) vers le système de fichiers.

> **Note**
>
> Si votre fonction n'est pas déjà connectée à un VPC, veuillez consulter Permettre à Lambda Event Functions d'accéder aux ressources d'un Amazon VPC.

Pour configurer l'accès au système de fichiers EFS

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez une fonction.
3. Sélectionnez Configuration, puis File systems (Systèmes de fichiers).
4. Sous Système de fichiers, choisissez Ajouter un système de fichiers.
5. Sélectionnez EFS.
6. Configurez les propriétés suivantes :
   - Système de fichiers EFS – Point d'accès d'un système de fichiers dans le même VPC.
   - Chemin de montage local – Emplacement où le système de fichiers est monté sur la fonction Lambda, commençant par `/mnt/`.

> **Tarification**
>
> Amazon EFS facture le stockage et le débit, avec des tarifs qui varient selon la classe de stockage. Pour plus d'informations, consultez Tarification Amazon EFS.
> Lambda facture le transfert de données entre VPC. Cela ne s'applique que si le VPC de votre fonction est appairé à un autre VPC avec un système de fichiers. Les tarifs sont les mêmes que pour le transfert de données Amazon EC2 entre VPC dans une même région. Pour plus d'informations, consultez Tarification ambda.

Régions prises en charge

Amazon EFS pour Lambda est disponible dans toutes les régions commerciales, à l'exception de l'Asie-Pacifique (Nouvelle Zélande), de l'Asie-Pacifique (Taipei), de l'Asie-Pacifique (Malaisie), de l'Asie-Pacifique (Thaïlande) et de l'Ouest du Canada (Calgary).

Configuration de l'accès aux fichiers Amazon S3

Amazon S3 Files fournit un système de fichiers partagé qui connecte n'importe quelle ressource de AWS calcul directement à vos données dans Amazon S3. Amazon S3 Files permet d'accéder à vos objets Amazon S3 sous forme de fichiers à l'aide d'opérations de système de fichiers standard telles que la lecture et l'écriture sur le chemin de montage local. En savoir plus sur Amazon S3 Files.

Sections

- Prérequis et configuration
- Rôle d’exécution et autorisations utilisateur
- Connexion à un système de fichiers (console)
- Configuration des lectures directes

Prérequis et configuration

Avant de configurer Amazon S3 Files avec votre fonction Lambda, assurez-vous de disposer des éléments suivants :

- Un système de fichiers Amazon S3 et des cibles de montage à l'état disponible dans le même compte et en Région AWS tant que fonction Lambda.
- Une fonction Lambda dans le même VPC que la cible de montage. Vous devez disposer d'une cible de montage dans chaque sous-réseau où votre fonction est déployée.
- Groupes de sécurité qui autorisent le trafic NFS (port 2049) entre votre fonction Lambda et les cibles de montage. En savoir plus sur la configuration des groupes de sécurité.

Pour plus d'informations, consultez les rubriques suivantes dans le guide de l'utilisateur Amazon S3 :

- Commencer à utiliser Amazon S3 Files
- Conditions préalables requises pour Amazon S3 Files
- Bonnes pratiques relatives aux fichiers Amazon S3

Rôle d’exécution et autorisations utilisateur

Le rôle d'exécution de votre fonction doit disposer des autorisations suivantes pour accéder à un système de fichiers Amazon S3 Files :

Autorisations du rôle d'exécution

- s3files : ClientMount — Nécessaire pour monter le système de fichiers.
- s3files : ClientWrite — Nécessaire pour l'accès en lecture-écriture. Inutile pour les connexions en lecture seule.

Ces autorisations sont incluses dans la politique AmazonS3FilesClientReadWriteAccessgérée. En outre, votre rôle d'exécution doit posséder leautorisations requises pour se connecter au VPC du système de fichiers.

> **Note**
>
> Amazon S3 Files optimise le débit en diffusant les demandes de lecture éligibles directement depuis votre compartiment Amazon S3. Les lectures directes sont activées par défaut pour les fonctions configurées avec 512 Mo de mémoire ou plus. Pour plus d'informations, consultez Configuration des lectures directes.

Votre fonction a également besoin des autorisations suivantes pour lire directement depuis Amazon S3 :

- s3 : GetObject
- s3 : GetObjectVersion

Pour plus d'informations sur les autorisations requises, consultez la section Autorisations IAM pour les fichiers Amazon S3 dans le guide de l'utilisateur Amazon S3.

Lorsque vous configurez un système de fichiers dans la console, Lambda utilise vos autorisations pour vérifier les cibles de montage et les points d'accès. Pour configurer une fonction pour vous connecter à un système de fichiers, votre utilisateur a besoin des autorisations suivantes :

Autorisations des utilisateurs

- Fichiers S3 : ListFileSystems
- Fichiers S3 : ListAccessPoints
- Fichiers S3 : GetFileSystem
- Fichiers S3 : GetAccessPoint

- s3files : CreateAccessPoint — Nécessaire si vous associez le système de fichiers à la fonction depuis la console.

L'exemple de politique suivant accorde à votre fonction des autorisations de rôle d'exécution lui permettant de monter un système de fichiers Amazon S3 avec un accès en lecture-écriture et en lecture directement depuis Amazon S3.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3FilesLambdaAccess",
            "Effect": "Allow",
            "Action": [
                "s3files:ClientMount",
                "s3files:ClientWrite"
            ],
            "Resource": "*"
        },
        {
            "Sid": "S3DirectRead",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": "arn:aws:s3:::bucket-name/*"
        },
        {
            "Sid": "S3FilesConsoleSetup",
            "Effect": "Allow",
            "Action": [
                "s3files:ListFileSystems",
                "s3files:ListAccessPoints",
                "s3files:GetFileSystem",
                "s3files:GetAccessPoint",
                "s3files:CreateAccessPoint"
            ],
            "Resource": "*"
        }
    ]
}
```

Connexion à un système de fichiers (console)

Une fonction se connecte à un système de fichiers sur le réseau local dans un VPC. Les sous-réseaux auquel votre fonction se connecte peuvent être les mêmes sous-réseaux qui contiennent des points de montage pour votre système de fichiers, ou des sous-réseaux de la même zone de disponibilité qui peuvent acheminer le trafic NFS (port 2049) vers le système de fichiers.

> **Note**
>
> Si votre fonction n'est pas déjà connectée à un VPC, veuillez consulter Permettre à Lambda Event Functions d'accéder aux ressources d'un Amazon VPC.

Pour configurer l'accès aux fichiers S3

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez une fonction.
3. Choisissez Configuration, puis Systèmes de fichiers.
4. Choisissez Ajouter un système de fichiers (ou Modifier pour modifier une configuration existante).
5. Sélectionnez S3 Files.
6. Configurez les propriétés suivantes :
   - Système de fichiers S3 — Choisissez un système de fichiers dans la liste déroulante.
   - Point d'accès (facultatif) — Choisissez un point d'accès. Si le système de fichiers ne possède aucun point d'accès, Lambda en crée un automatiquement lors de l'enregistrement (UID/GID 1000:1000, répertoire `/lambda` racine, autorisations 755). S'il existe des points d'accès, vous devez en sélectionner un.
   - Chemin de montage local – Emplacement où le système de fichiers est monté sur la fonction Lambda, commençant par `/mnt/`.
   - Configuration avancée
     - Lectures S3 directes : contrôle si Lambda peut diffuser des lectures éligibles directement depuis votre compartiment Amazon S3 pour un débit plus élevé. Pour plus d'informations, consultez Configuration des lectures directes.
7. Cliquez sur Enregistrer.

Votre système de fichiers est attaché la prochaine fois que vous appelez votre fonction Lambda.

Configuration des lectures directes

Les lectures directes optimisent le débit en diffusant des données directement depuis votre compartiment Amazon S3. Lambda utilise des lectures directes pour les lectures volumineuses et lorsque le stockage haute performance du système de fichiers ne contient pas les données des fichiers. Pour plus d'informations, consultez Comment S3 Files fournit des performances. Cette configuration facultative fait partie `FileSystemConfigs` de votre fonction et s'applique uniquement aux systèmes de fichiers Amazon S3. Le `DirectS3Read` paramètre accepte les valeurs suivantes :

- `AUTO`(par défaut) — Active la lecture directe pour les fonctions configurées avec 512 Mo de mémoire ou plus.
- `ENABLED`— Permet la lecture directe de votre fonction, y compris les fonctions avec moins de 512 Mo de mémoire.
- `DISABLED`— Achemine toutes les lectures via le stockage haute performance du système de fichiers.

> **Note**
>
> Si une lecture directe échoue, Lambda recommence automatiquement à lire dans le système de fichiers.

Pour utiliser les lectures directes, le rôle d'exécution de votre fonction doit disposer des autorisations requises. Pour plus d'informations, consultez les politiques prérequises d'Amazon S3 Files.

Création d'un alias pour une fonction d'événement Lambda

Vous pouvez créer des alias pour votre fonction Lambda. Un alias Lambda est un pointeur vers une version de la fonction que vous pouvez mettre à jour. Les utilisateurs de la fonction peuvent accéder à la version de la fonction en utilisant l'alias Amazon Resource Name (ARN). Lorsque vous déployez une nouvelle version, vous pouvez mettre à jour l'alias pour utiliser la nouvelle version, ou diviser le trafic entre deux versions. Pour plus d'informations sur l'utilisation d'alias dans vos applications, consultezthe section called “Utilisation des alias”.

Console

Pour créer un alias à l’aide de la console

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez une fonction.
3. Sélectionnez Alias, puis Create alias (Créer un alias).
4. Sur la page Create alias (Créer un alias), procédez de la manière suivante :
   a. Renseignez le champ Name (Nom) pour l'alias.
   b. (Facultatif) Renseignez le champ Description de l'alias.
   c. Pour Version, choisissez une version de fonction vers laquelle vous souhaitez que l'alias pointe.
   d. (Facultatif) Pour configurer le routage sur l'alias, développez Weighted alias (Alias pondéré). Pour de plus amples informations, veuillez consulter Mise en œuvre de déploiements canary Lambda à l’aide d’un alias pondéré.
   e. Cliquez sur Enregistrer.

AWS CLI

Pour créer un alias à l'aide de AWS Command Line Interface (AWS CLI), utilisez la commande create-alias.

```
aws lambda create-alias \
  --function-name my-function \
  --name alias-name \
  --function-version version-number \
  --description " "
```

Pour modifier un alias afin qu'il pointe vers une nouvelle version de la fonction, utilisez la commande update-alias.

```
aws lambda update-alias \
  --function-name my-function \
  --name alias-name \
  --function-version version-number
```

Pour créer un alias, utilisez la commande delete-alias.

```
aws lambda delete-alias \
  --function-name my-function \
  --name alias-name
```

Les AWS CLI commandes des étapes précédentes correspondent aux opérations d'API Lambda suivantes :

- CreateAlias
- UpdateAlias
- DeleteAlias

Utilisation d’alias Lambda dans les sources d’événements et les politiques d’autorisation

Chaque alias possède un ARN unique. Un alias peut uniquement pointer vers une version de fonction, et non vers un autre alias. Vous pouvez mettre à jour un alias de sorte qu’il pointe vers une nouvelle version de la fonction.

Des sources d'événements telles qu'Amazon Simple Storage Service (Amazon S3) appellent votre fonction Lambda. Ces sources d'événements gèrent un mappage qui identifie la fonction à appeler lorsque des événements se produisent. Si vous spécifiez un alias de fonction Lambda dans la configuration du mappage, vous n'avez pas besoin de mettre à jour le mappage lorsque la version de la fonction change. Pour de plus amples informations, veuillez consulter Procédure de traitement par Lambda des enregistrements provenant de sources d’événements basées sur des flux et des files d’attente.

Dans une stratégie de ressources, vous pouvez accorder des autorisations en lien avec des sources d'événements à utiliser votre fonction Lambda. Si vous spécifiez un ARN d'alias dans la stratégie, vous n'avez pas besoin de mettre à jour la stratégie lorsque la version de la fonction change.

Stratégies basées sur une ressource

Vous pouvez utiliser une stratégie basée sur les ressources pour accorder l'accès à votre fonction à un service, à une ressource ou à un compte. La portée de cette autorisation est dépendante du fait que vous appliquiez l'autorisation à un alias, à une version ou à la fonction entière. Par exemple, si vous utilisez un nom d'alias (tel que`helloworld:PROD`), vous pouvez invoquer la `helloworld` fonction à l'aide de l'alias ARN (`helloworld:PROD`).

Si vous essayez d'appeler la fonction sans alias ou version spécifique, vous obtenez une erreur d'autorisation. Cette erreur d'autorisation continue de se produire même si vous tentez d'appeler directement la version de fonction associée à l'alias.

Par exemple, la AWS CLI commande suivante accorde à Amazon S3 les autorisations nécessaires pour invoquer l'alias PROD de la `helloworld` fonction lorsqu'Amazon S3 agit pour le compte de. `amzn-s3-demo-bucket`

```
aws lambda add-permission \
  --function-name helloworld \
  --qualifier PROD \
  --statement-id 1 \
```

```
  --principal s3.amazonaws.com \
  --action lambda:InvokeFunction \
  --source-arn arn:aws:s3:::amzn-s3-demo-bucket \
  --source-account 123456789012
```

Pour de plus amples informations sur l'utilisation des noms de ressources dans les stratégies, veuillez consulter Fine-tuning les sections Ressources et Conditions des politiques.

Mise en œuvre de déploiements canary Lambda à l'aide d'un alias pondéré

Vous pouvez utiliser un alias pondéré pour répartir le trafic entre deux versions différentes de la même fonction. Cette approche vous permet de tester de nouvelles versions de vos fonctions avec un faible pourcentage de trafic et de revenir rapidement en arrière si nécessaire. C'est ce que l'on appelle un déploiement canary. Les déploiements Canary diffèrent blue/green des déploiements en exposant la nouvelle version à une partie seulement des demandes plutôt que de changer tout le trafic en une seule fois.

Vous pouvez faire pointer un alias vers au maximum deux versions de fonction Lambda. Les versions doivent répondre aux critères suivants :

- Les deux versions doivent avoir le même rôle d'exécution.
- Les deux versions doivent avoir la même configuration de file d'attente de lettres mortes ou aucune configuration de file d'attente de lettres mortes.
- Les deux versions doivent être publiées. L'alias ne peut pas pointer vers `$LATEST`.

> **Note**
>
> Lambda utilise un modèle probabiliste simple pour distribuer le trafic entre les deux versions de la fonction. Quand le niveau de trafic est faible, il se peut que vous observiez une variance élevée entre les pourcentages de trafic configuré et réel sur chaque version. Si votre fonction utilise une simultanéité approvisionnée, vous pouvez éviter des invocations de débordement en configurant un plus grand nombre d'instances de simultanéité approvisionnées pendant que le routage d'alias est actif.

Création d'un alias pondéré

Console

Pour configurer le routage sur un alias à l'aide de la console

> **Note**
>
> Vérifiez que la fonction a au moins deux versions publiées. Pour créer des versions supplémentaires, suivez les instructions de la section Création de versions de fonction.

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez une fonction.
3. Sélectionnez Alias, puis Create alias (Créer un alias).
4. Sur la page Create alias (Créer un alias), procédez de la manière suivante :
   a. Renseignez le champ Name (Nom) pour l'alias.
   b. (Facultatif) Renseignez le champ Description de l'alias.
   c. Pour Version, choisissez la première version de fonction vers laquelle vous souhaitez que l'alias pointe.
   d. Développez Weighted alias (Alias pondéré).
   e. Pour Additional version (Version supplémentaire), choisissez la deuxième version de fonction vers laquelle vous souhaitez que l'alias pointe.
   f. Pour Weight (%) (Pondération (%)), entrez une valeur de pondération pour la fonction. La pondération est le pourcentage de trafic qui est affecté à cette version lorsque l'alias est appelé. La première version reçoit le reste du trafic. Par exemple, si vous spécifiez 10 % pour Additional version (Version supplémentaire), 90 % du trafic est automatiquement affecté à la première version.
   g. Choisissez Enregistrer.

AWS CLI

Utilisez les AWS CLI commandes create-alias et update-alias pour configurer les pondérations du trafic entre deux versions de fonction. Lorsque vous créez ou mettez à jour l'alias, vous spécifiez la pondération du trafic dans le paramètre `routing-config`.

L'exemple suivant crée un alias de fonction Lambda nommé routing-alias qui pointe vers la version 1 de la fonction. La version 2 de la fonction reçoit 3 % du trafic. Les 97 % restants du trafic sont acheminés vers la version 1.

```
aws lambda create-alias \
  --name routing-alias \
  --function-name my-function \
  --function-version 1  \
  --routing-config AdditionalVersionWeights={"2"=0.03}
```

Utilisez la commande `update-alias` pour augmenter le pourcentage de trafic entrant vers la version 2. Dans l'exemple suivant, vous augmentez le trafic à 5 %.

```
aws lambda update-alias \
  --name routing-alias \
  --function-name my-function \
  --routing-config AdditionalVersionWeights={"2"=0.05}
```

Pour acheminer l'ensemble du trafic vers la version 2, utilisez la commande `update-alias` pour modifier la propriété `function-version` afin que l'alias pointe vers la version 2. La commande réinitialise également la configuration de routage.

```
aws lambda update-alias \
  --name routing-alias \
  --function-name my-function  \
  --function-version 2 \
  --routing-config AdditionalVersionWeights={}
```

Les AWS CLI commandes des étapes précédentes correspondent aux opérations d'API Lambda suivantes :

- CreateAlias
- UpdateAlias

Détermination de la version invoquée

Lorsque vous configurez des pondérations de trafic entre deux versions de fonction, vous pouvez déterminer la version de fonction Lambda appelée de deux manières :

- CloudWatch Journaux — Lambda émet automatiquement une entrée de `START` journal contenant l'ID de version invoqué pour chaque appel de fonction. Exemple :

  ```
  START RequestId: 1dh194d3759ed-4v8b-a7b4-1e541f60235f Version: 2
  ```

  Pour les appels d'alias, Lambda utilise la dimension `ExecutedVersion` pour filtrer les métriques en fonction de la version appelée. Pour plus d'informations, consultez Affichage des métriques pour les fonctions d'événement Lambda.
- Charge utile de réponse (appels synchrones) – Les réponses aux appels de fonction synchrones incluent un en-tête `x-amz-executed-version` indiquant la version de fonction appelée.

Création d'un déploiement continu avec des alias pondérés

Utilisez AWS CodeDeploy and AWS Serverless Application Model (AWS SAM) pour créer un déploiement continu qui détecte automatiquement les modifications apportées à votre code de fonction, déploie une nouvelle version de votre fonction et augmente progressivement le volume de trafic vers la nouvelle version. La quantité de trafic et le taux d'augmentation sont des paramètres que vous pouvez configurer.

Dans le cadre d'un déploiement continu, AWS SAM exécute les tâches suivantes :

- Il configure votre fonction Lambda et crée un alias. La configuration de routage d'alias pondéré est la capacité sous-jacente qui implémente le déploiement propagé.
- Crée une CodeDeploy application et un groupe de déploiement. Le groupe de déploiement gère le déploiement propagé et la restauration, si nécessaire.
- Il détecte le moment où vous créez une nouvelle version de votre fonction Lambda.
- Déclencheurs CodeDeploy permettant de démarrer le déploiement de la nouvelle version.

Exemple AWS SAM modèle

L'exemple suivant présente un modèle AWS SAM pour un déploiement propagé simple.

```
AWSTemplateFormatVersion : '2010-09-09'
Transform: AWS::Serverless-2016-10-31
Description: A sample SAM template for deploying Lambda functions

Resources:
# Details about the myDateTimeFunction Lambda function
```

```
  myDateTimeFunction:
    Type: AWS::Serverless::Function
    Properties:
      Handler: myDateTimeFunction.handler
      Runtime: nodejs24.x
# Creates an alias named "live" for the function, and automatically publishes when you
 update the function.
      AutoPublishAlias: live
      DeploymentPreference:
# Specifies the deployment configuration
          Type: Linear10PercentEvery2Minutes
```

Ce modèle définit une fonction Lambda nommée `myDateTimeFunction` avec les propriétés suivantes.

AutoPublishAlias

La propriété `AutoPublishAlias` crée un alias nommé `live`. De plus, l'infrastructure AWS SAM détecte automatiquement le moment où vous enregistrez du code nouveau pour la fonction. L'infrastructure publie ensuite une nouvelle version de fonction et met à jour l'alias `live` de sorte qu'il pointe vers la nouvelle version.

DeploymentPreference

La `DeploymentPreference` propriété détermine la vitesse à laquelle l' CodeDeploy application déplace le trafic de la version d'origine de la fonction Lambda vers la nouvelle version. La valeur `Linear10PercentEvery2Minutes` déplace 10 % supplémentaires du trafic vers la nouvelle version toutes les 2 minutes.

Pour obtenir la liste des configurations de déploiement prédéfinies, consultez Configurations de déploiement.

Pour plus d'informations sur la façon de créer des déploiements progressifs avec CodeDeploy et AWS SAM, consultez les rubriques suivantes :

- Tutoriel : Déployer une fonction Lambda mise à jour avec et CodeDeploy AWS Serverless Application Model
- Déploiement progressif d'applications sans serveur avec AWS SAM

Gérer les versions de la fonction d'événement Lambda

Vous pouvez utiliser les versions pour gérer le déploiement de vos fonctions . Par exemple, vous pouvez publier une nouvelle version d'une fonction à des fins de test bêta sans affecter les utilisateurs de la version de production stable. Lambda crée une nouvelle version de votre fonction chaque fois que vous la publiez. La nouvelle version est une copie de la version non publiée de la fonction. La version non publiée est nommée `$LATEST`.

Il est important de noter que chaque fois que vous déployez le code de votre fonction, vous remplacez le code actuel dans `$LATEST`. Pour enregistrer l'itération `$LATEST` actuelle, créez une nouvelle version de la fonction. Si `$LATEST` est identique à une version publiée précédemment, aucune nouvelle version ne pourra être créée tant que les modifications n'auront pas été déployées dans `$LATEST`. Ces modifications peuvent inclure la mise à jour du code ou la modification des paramètres de configuration de la fonction.

Une fois que vous avez publié une version de fonction, son code, son environnement d'exécution, son architecture, sa mémoire, ses couches et la plupart des autres paramètres de configuration sont immuables. Cela signifie que vous ne pouvez pas modifier ces paramètres sans publier une nouvelle version à partir de `$LATEST`. Vous pouvez configurer les éléments suivants pour une version de fonction publiée :

- Déclencheurs
- Destinations
- Simultanéité allouée
- invocation asynchrone
- Connexions aux bases de données et proxys

> **Note**
>
> Lorsque vous utilisez les contrôles de gestion de l'environnement d'exécution avec le mode Auto, la version de l'environnement d'exécution utilisée par la version de la fonction est mise à jour automatiquement. Lorsque vous utilisez le mode Function update (Mise à jour de fonction) ou Manual (Manuel), la version de l'environnement d'exécution n'est pas mise à jour. Pour plus d'informations, consultez the section called "Mises à jour de version de l'environnement d'exécution".

Sections

- Création de versions de fonction
- Utilisation des versions
- Octroi d'autorisations

Création de versions de fonction

Vous pouvez modifier le code et les paramètres de la fonction uniquement sur la version non publiée d'une fonction. Lorsque vous publiez une version, Lambda verrouille le code et la plupart des paramètres afin de préserver une expérience cohérente pour les utilisateurs de cette version.

Vous pouvez créer une version de fonction à l'aide de la console Lambda.

Pour créer une version de fonction

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez une fonction, puis choisissez l'onglet Versions.
3. Sur la page de configuration des versions, sélectionnez Publish new version (Publier une nouvelle version).
4. (Facultatif) Entrez une description de la version.
5. Choisissez Publier.

Vous pouvez également publier une version d'une fonction à l'aide de l'opération PublishVersionAPI.

La AWS CLI commande suivante publie une nouvelle version d'une fonction. La réponse renvoie les informations de configuration relatives à la nouvelle version, y compris le numéro de version et l'ARN de la fonction avec le suffixe de version.

```
aws lambda publish-version --function-name my-function
```

Vous devriez voir la sortie suivante :

```
{
  "FunctionName": "my-function",
  "FunctionArn": "arn:aws:lambda:us-east-2:123456789012:function:my-function:1",
  "Version": "1",
```

```
  "Role": "arn:aws:iam::123456789012:role/lambda-role",
  "Handler": "function.handler",
  "Runtime": "nodejs24.x",
  ...
}
```

> **Note**
>
> Lambda attribue des numéros de séquence à croissance monotone pour la gestion des versions. Lambda ne réutilise jamais les numéros de version, même après avoir supprimé et recréé une fonction.

Utilisation des versions

Vous pouvez référencer votre fonction Lambda à l'aide d'un ARN qualifié ou d'un ARN non qualifié.

- ARN qualifié – ARN de la fonction avec suffixe de version. L'exemple suivant fait référence à la version 42 de la fonction `helloworld`.

  ```
  arn:aws:lambda:aws-region:acct-id:function:helloworld:42
  ```

- ARN non qualifié – ARN de la fonction sans suffixe de version.

  ```
  arn:aws:lambda:aws-region:acct-id:function:helloworld
  ```

Vous pouvez utiliser un ARN qualifié ou non qualifié dans toutes les opérations d'API pertinentes. Cependant, vous ne pouvez pas utiliser un ARN non qualifié pour créer un alias.

Si vous décidez de ne pas publier de versions de fonction, vous pouvez invoquer la fonction à l'aide de l'ARN qualifié ou non qualifié dans votre mappage source d'événement. Lorsque vous invoquez une fonction à l'aide d'un ARN non qualifié, Lambda invoque implicitement `$LATEST`.

L'ARN qualifié pour chaque version de fonction Lambda est unique. Après avoir publié une version, vous ne pouvez pas modifier l'ARN ou le code de fonction.

Lambda ne publie une nouvelle version de fonction que si le code n'a jamais été publié ou si le code a changé par rapport à la version publiée la plus récente. S'il n'y a pas de changement, la version de fonction publiée la plus récente reste active.

Lorsque vous publiez une version, Lambda crée un instantané immuable du code et de la configuration de votre fonction. Les modifications de configuration ne déclenchent pas toutes la publication d'une nouvelle version. Les modifications de configuration suivantes rendent une fonction éligible à la publication d'une nouvelle version :

- Code de fonction
- Variables d'environnement
- Environnement d'exécution
- Handler (Gestionnaire)
- Layers
- Taille de la mémoire
- Timeout
- Configuration VPC
- Configuration de file d'attente de lettres mortes (DLQ)
- Rôle IAM
- Description
- Architecture (x86_64 ou arm64)
- Taille du stockage éphémère
- Type de package
- Mode de stockage de code (commutation entre le stockage S3 autogéré Lambda-managed et le stockage S3)
- Configuration de la journalisation
- Configuration du système de fichiers
- SnapStart
- Configuration du suivi

Les paramètres opérationnels, comme la simultanéité réservée, ne déclenchent pas la publication d'une nouvelle version lorsqu'ils sont modifiés.

Octroi d'autorisations

Vous pouvez utiliser une stratégie basée sur les ressources ou une stratégie basée sur l'identité pour accorder l'accès à votre fonction. La portée de l'autorisation est dépendante du fait que

vous appliquiez la stratégie à une fonction ou à une version d’une fonction. Pour de plus amples informations sur les noms de ressource de fonction dans les stratégies, veuillez consulter Fine-tuning les sections Ressources et Conditions des politiques.

Vous pouvez simplifier la gestion des sources d'événements et des politiques Gestion des identités et des accès AWS (IAM) en utilisant des alias de fonction. Pour plus d'informations, consultez Création d'un alias pour une fonction d'événement Lambda.

Utilisation de balises sur les fonctions d'événement Lambda

Vous pouvez étiqueter les fonctions pour organiser et gérer vos ressources. Les balises sont des paires clé-valeur de forme libre associées à vos ressources prises en charge par l'ensemble des ressources Services AWS. Pour plus d'informations sur les cas d'utilisation des balises, consultez la section Stratégies de balisage courantes dans le guide des AWS ressources de balisage et de l'éditeur de balises.

Les balises s'appliquent au niveau de la fonction, pas aux versions ni aux alias. Les balises ne font pas partie de la configuration spécifique à la version qui AWS Lambda crée un instantané du moment où vous publiez une version. Vous pouvez utiliser l'API Lambda pour afficher et mettre à jour les balises. Vous pouvez également afficher et mettre à jour les balises tout en gérant une fonction spécifique dans la console Lambda.

Vous pouvez également utiliser des balises pour contrôler l'accès à vos fonctions grâce au contrôle d'accès basé sur les attributs (ABAC). Pour plus d'informations, consultez the section called "Attribute-based contrôle d'accès".

Sections

- Autorisations requises pour l'utilisation des balises
- Utilisation des balises avec la console Lambda
- Utilisation de balises avec le AWS CLI

Autorisations requises pour l'utilisation des balises

Pour autoriser une identité Gestion des identités et des accès AWS (IAM) – utilisateur, groupe ou rôle – à afficher ou marquer les ressources, accordez-lui les autorisations correspondantes :

- lambda : ListTags —Lorsqu' une ressource possède des balises, accordez cette autorisation à tous ceux qui ont besoin de `ListTags` l'utiliser. Pour les fonctions d'événement balisées, cette autorisation est également nécessaire pour`GetFunction`.
- lambda : TagResource —Accordez cette autorisation à toute personne ayant besoin d'appeler `TagResource` ou d'exécuter un tag lors de la création.

Vous pouvez éventuellement envisager d'accorder également l'UntagResourceautorisation lambda : pour autoriser les `UntagResource` appels à la ressource.

Pour plus d'informations, consultez Identity-based Politiques IAM pour Lambda.

Utilisation des balises avec la console Lambda

Vous pouvez utiliser la console Lambda pour créer des fonctions qui comportent des balises, pour ajouter des balises aux fonctions existantes et pour filtrer des fonctions selon les balises ajoutées.

Ajout de balises lors de la création d'une fonction

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez Create Event Function.
3. Choisissez Author from scratch (Créer à partir de zéro) ou Container image (Image de conteneur).
4. Sous Informations de base, configurez votre fonction. Pour de plus amples informations sur la configuration des fonctions, consultez the section called "Configuration des fonctions événementielles".
5. Développez Advanced settings (Paramètres avancés) et sélectionnez Enable tags (Activer les balises).
6. Pour cela, choisissez Ajouter une balise, puis saisissez une clé et éventuellement une valeur. Répétez cette étape pour ajouter d'autres balises.
7. Choisissez Create Event Function.

Pour ajouter des balises à une fonction existante

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez le nom d'une fonction.
3. Sélectionnez Configuration, puis Tags (Balises).
4. Sous Balises, choisissez Gérer les balises.
5. Pour cela, choisissez Ajouter une balise, puis saisissez une clé et éventuellement une valeur. Répétez cette étape pour ajouter d'autres balises.
6. Cliquez sur Enregistrer.

Pour filtrer des fonctions avec des balises

1. Ouvrez la page Event Functions de la console Lambda.

2. Cliquez dans la zone de recherche pour afficher la liste des propriétés de fonction et des clés de balise.
3. Choisissez une clé de balise pour voir la liste des valeurs utilisées dans la AWS région actuelle.
4. Sélectionnez Utiliser : « tag-name » pour afficher toutes les fonctions étiquetées avec cette touche, ou choisissez un Opérateur pour affiner le filtrage en fonction de la valeur.
5. Sélectionnez votre valeur de balise pour appliquer un filtre combinant la clé et la valeur de la balise.

La barre de recherche prend également en charge la recherche de clés de balise. Saisissez `tag` pour afficher uniquement une liste de clés de balise ou entrez le nom d'une clé pour la rechercher dans la liste.

Utilisation de balises avec le AWS CLI

Vous pouvez ajouter et supprimer des balises sur les ressources Lambda existantes, fonctions incluses, avec l'API Lambda. Vous pouvez également ajouter des balises lors de la création d'une fonction, afin de conserver une ressource étiquetée tout au long de son cycle de vie.

Mise à jour des balises avec les API de balises Lambda

Vous pouvez ajouter et supprimer des balises pour les ressources Lambda prises en charge par le biais des opérations TagResourceet de l'UntagResourceAPI.

Vous pouvez appeler ces opérations par l'intermédiaire de l' AWS CLI. Pour ajouter des balises à une ressource existante, utilisez la commande `tag-resource`. Cet exemple ajoute deux balises, l'une avec la clé *`Department`* et l'autre avec la clé*`CostCenter`*.

```
aws lambda tag-resource \
--resource arn:aws:lambda:us-east-2:123456789012:resource-type:my-resource \
--tags Department=Marketing,CostCenter=1234ABCD
```

Pour supprimer des balises, utilisez la commande `untag-resource`. Cet exemple supprime la balise contenant la clé*`Department`*.

```
aws lambda untag-resource --resource arn:aws:lambda:us-east-1:123456789012:resource-
type:resource-identifier \
--tag-keys Department
```

Ajout de balises lors de la création d'une fonction

Pour créer une nouvelle fonction Lambda avec des balises, utilisez l'opération CreateFunctionAPI. Spécifiez le paramètre `Tags`. Vous pouvez appeler cette opération à l'aide de la commande `create-function` de la CLI associée à l'option --tags.

Avant d'utiliser le paramètre tags avec `CreateFunction`, vérifiez que votre rôle dispose de l'autorisation de baliser les ressources en plus des autorisations habituelles nécessaires à cette opération. Pour plus d'informations sur les autorisations requises pour l'étiquetage, consultez the section called "Autorisations requises pour l'utilisation des balises". Cet exemple ajoute deux balises, l'une avec la clé *`Department`* et l'autre avec la clé*`CostCenter`*.

```
aws lambda create-function --function-name my-function
--handler index.js --runtime nodejs24.x \
--role arn:aws:iam::123456789012:role/lambda-role \
--tags Department=Marketing,CostCenter=1234ABCD
```

Affichage des balises d'une fonction

Pour afficher les balises associées à une ressource Lambda spécifique, utilisez l'opération d'API `ListTags`. Pour plus d'informations, consultez ListTags.

Vous pouvez appeler cette opération à l'aide de la `list-tags` AWS CLI commande en fournissant un ARN (Amazon Resource Name).

```
aws lambda list-tags --resource arn:aws:lambda:us-east-1:123456789012:resource-
type:resource-identifier
```

Vous pouvez afficher les balises appliquées à une ressource spécifique à l'aide de l'opération GetFunctiond'API. Aucune fonctionnalité comparable n'est disponible pour les autres types de ressources.

Vous pouvez appeler cette opération à l'aide de la commande `get-function` de la CLI :

```
aws lambda get-function --function-name my-function
```

Filtrage de ressources par balise

Vous pouvez utiliser l'opération AWS Resource Groups Tagging API GetResourcesAPI pour filtrer vos ressources par balises. L'opération `GetResources` reçoit jusqu'à 10 filtres, chaque filtre

contenant une clé de balise et jusqu'à 10 valeurs de balise. Vous fournissez `GetResources`avec un `ResourceType` pour filtrer par certains types de ressources.

Vous pouvez appeler cette opération à l'aide de la `get-resources` AWS CLI commande. Pour des exemples d'utilisation de `get-resources`, consultez get-resources dans la Référence des commandes de l'AWS CLI.

Streaming de réponses pour les fonctions d'événement Lambda

Les fonctions Lambda peuvent renvoyer nativement les charges utiles de réponse aux clients via les URL des fonctions Lambda ou à l'aide de l'InvokeWithResponseStreamAPI (via le SDK ou des appels d'API directs). AWS Votre fonction Lambda peut également diffuser des charges utiles de réponse via l'intégration du proxy Amazon API Gateway, qui utilise l'InvokeWithResponseStreamAPI pour appeler votre fonction. Le streaming de réponses peut profiter aux applications sensibles à la latence en améliorant les performances de temps au premier octet (TTFB). En effet, vous pouvez renvoyer des réponses partielles au client dès qu'elles sont disponibles. En outre, les fonctions de diffusion des réponses peuvent renvoyer des données utiles allant jusqu'à 200 Mo, contre un maximum de 6 Mo pour les réponses mises en mémoire tampon.

Le streaming d'une réponse signifie également que votre fonction n'a pas besoin de mémoriser l'intégralité de la réponse. Pour les réponses très volumineuses, cela peut réduire la quantité de mémoire que vous devez configurer pour votre fonction. Pour vous aider à choisir entre les URL des fonctions et API Gateway pour votre cas d'utilisation, consultezthe section called "URL de fonction et Amazon API Gateway".

> **Note**
>
> Le streaming des réponses Lambda n'est pas encore disponible dans tous les cas. Régions AWS Pour connaître la disponibilité des fonctionnalités par région, consultez la section AWS Capacités par région du Builder Center.

La vitesse à laquelle Lambda diffuse vos réponses dépend de la taille de la réponse. Le débit de diffusion pour les 6 premiers Mo de réponse de votre fonction n'est pas plafonné. Pour les réponses supérieures à 6 Mo, le reste de la réponse est soumis à une limite de bande passante. Pour plus d'informations sur la bande passante de diffusion, consultez Limitation de la bande passante pour la diffusion des réponses.

Les réponses en streaming entraînent des coûts et les réponses diffusées en continu ne sont ni interrompues ni arrêtées lorsque la connexion du client appelant est interrompue. Les clients sont facturés pour la durée complète des fonctions. Ils doivent donc faire preuve de prudence lorsqu'ils configurent des délais d'expiration de fonction prolongés.

Lambda prend en charge le streaming des réponses sur les environnements d'exécution Node.js gérés. Pour les autres langages, y compris Python, vous pouvez utiliser un environnement

d'exécution personnalisé avec une intégration d'API d'exécution personnalisée pour diffuser les réponses ou utiliser l'adaptateur Web Lambda.

> **Note**
>
> Lorsque vous testez votre fonction via la console Lambda, vous verrez toujours les réponses comme étant mises en mémoire tampon.

Pour savoir comment écrire des fonctions de streaming, voirthe section called “Écriture de fonctions”. Pour appeler des fonctions de streaming via des URL de fonctions, consultezthe section called “Invocation de fonctions”. Pour une procédure pas à pas, voirthe section called “Tutoriel : création d’une fonction de streaming de réponses avec une URL de la fonction”.

Rubriques

- Limitation de la bande passante pour la diffusion des réponses
- Compatibilité du VPC avec la diffusion en continu de réponses
- Écriture de fonctions Lambda compatibles avec le streaming de réponses
- Invocation d’une fonction compatible avec le flux de réponses à l’aide des URL de fonctions Lambda
- Tutoriel : création d’une fonction Lambda de streaming de réponses avec une URL de la fonction

Limitation de la bande passante pour la diffusion des réponses

Les 6 premiers Mo de la charge utile de réponse de votre fonction ont une bande passante illimitée. Après cette première salve, Lambda diffuse votre réponse à un débit maximum de 2 Mbit/s. Si les réponses de votre fonction ne dépassent jamais 6 Mo, cette limite de bande passante ne s’applique pas.

> **Note**
>
> Les limites de bande passante ne s'appliquent qu'à la charge utile de réponse de votre fonction, et non à l'accès au réseau par votre fonction.

Le taux de bande passante non plafonnée varie en fonction d'un certain nombre de facteurs, notamment la vitesse de traitement de votre fonction. Vous pouvez normalement vous attendre à un

débit supérieur à 2 Mbits/s pour les 6 premiers Mo de réponse de votre fonction. Si votre fonction diffuse une réponse vers une destination située à l'extérieur AWS, le débit de diffusion dépend également de la vitesse de la connexion Internet externe.

Compatibilité du VPC avec la diffusion en continu de réponses

Lorsque vous utilisez des fonctions Lambda dans un environnement VPC, la diffusion en continu des réponses doit tenir compte de certaines considérations importantes :

- Les URL des fonctions Lambda ne prennent pas en charge la diffusion en continu des réponses dans un environnement VPC.
- Vous pouvez utiliser le streaming de réponses au sein d'un VPC en appelant votre fonction Lambda via le SDK à l'aide de l' AWS API. `InvokeWithResponseStream` Pour cela, vous devez configurer les points de terminaison VPC appropriés pour Lambda.
- Pour les environnements VPC, vous devez créer un point de terminaison de VPC d’interface pour Lambda afin de permettre la communication entre vos ressources dans le VPC et dans le service Lambda.

Une architecture typique pour la diffusion en continu des réponses dans un VPC peut inclure :

```
Client in VPC -> Interface VPC endpoint for Lambda -> Lambda function -> Response
 streaming back through the same path
```

Écriture de fonctions Lambda compatibles avec le streaming de réponses

L'écriture du gestionnaire pour les fonctions de streaming de réponses est différente des modèles de gestionnaire typiques. Lorsque vous écrivez des fonctions de streaming, assurez-vous de faire ce qui suit :

- Encapsulez votre événement avec le décorateur `awslambda.streamifyResponse()`. L’objet global `awslambda` est fourni par l’environnement d’exécution Node.js de Lambda.
- Terminez la diffusion de manière élégante afin de vous assurer que le traitement des données est terminé.

Configuration d'une fonction gestionnaire pour diffuser les réponses

Pour indiquer à l'exécution que Lambda doit diffuser les réponses de votre fonction, vous devez envelopper votre fonction avec le décorateur `streamifyResponse()`. Cela indique à l'exécution

d'utiliser le chemin logique approprié pour le streaming des réponses et permet à la fonction de diffuser les réponses.

Le décorateur `streamifyResponse()` accepte une fonction qui accepte les paramètres suivants :

- `event` : fournit des informations sur l'événement d'invocation de l'URL de la fonction, telles que la méthode HTTP, les paramètres de la requête et le corps de la requête.
- `responseStream` : fournit un flux inscriptible.
- `context` : fournit des méthodes et des propriétés avec des informations sur l'invocation, la fonction et l'environnement d'exécution.

L'objet `responseStream` est un `writableStream` Node.js. Comme pour tout flux de ce type, vous devez utiliser la méthode `pipeline()`.

> **Note**
>
> L'objet global `awslambda` est automatiquement fourni par l'environnement d'exécution Node.js de Lambda et aucune importation n'est requise.

Example gestionnaire compatible avec le streaming de réponses

```
import { pipeline } from 'node:stream/promises';
import { Readable } from 'node:stream';

export const echo = awslambda.streamifyResponse(async (event, responseStream, _context)
 => {
  // As an example, convert event to a readable stream.
  const requestStream = Readable.from(Buffer.from(JSON.stringify(event)));

  await pipeline(requestStream, responseStream);
});
```

Bien que `responseStream` propose la méthode `write()` pour écrire dans le flux, nous vous recommandons d'utiliser `pipeline()` dans la mesure du possible. L'utilisation de `pipeline()` permet de s'assurer que le flux accessible en écriture n'est pas submergé par un flux accessible en lecture plus rapide.

Fin du flux

Assurez-vous de terminer correctement le flux avant le retour du gestionnaire. La méthode `pipeline()` s'en charge automatiquement.

Pour les autres cas d'utilisation, appelez la méthode `responseStream.end()` pour terminer correctement un flux. Cette méthode signale que plus aucune donnée ne doit être écrite dans le flux. Cette méthode n'est pas nécessaire si vous écrivez dans le flux avec `pipeline()` ou `pipe()`.

À partir de Node.js 24, Lambda n'attend plus que les promesses non résolues se terminent après le retour de votre gestionnaire ou la fin du flux de réponses. Si votre fonction dépend d'opérations asynchrones supplémentaires, telles que des temporisations ou des extractions, vous devez `await` les inclure dans votre gestionnaire.

Example Exemple de fin d'un flux avec pipeline()

```
import { pipeline } from 'node:stream/promises';

export const handler = awslambda.streamifyResponse(async (event, responseStream,
 _context) => {
  await pipeline(requestStream, responseStream);
});
```

Example Exemple de fin d'un flux sans pipeline()

```
export const handler = awslambda.streamifyResponse(async (event, responseStream,
 _context) => {
  responseStream.write("Hello ");
  responseStream.write("world ");
  responseStream.write("from ");
  responseStream.write("Lambda!");
  responseStream.end();
});
```

Invocation d'une fonction compatible avec le flux de réponses à l'aide des URL de fonctions Lambda

> **Note**
>
> Votre fonction Lambda peut désormais diffuser les charges utiles des réponses via l'intégration du proxy Amazon API Gateway.

Vous pouvez invoquer des fonctions compatibles avec le streaming de réponses en modifiant le mode d'invocation de l'URL de votre fonction. Le mode d'invocation détermine l'opération d'API que Lambda utilise pour invoquer votre fonction. Les modes d'invocation disponibles sont les suivants :

- `BUFFERED` : il s'agit de l'option par défaut. Lambda invoque votre fonction en utilisant l'opération d'API `Invoke`. Les résultats de l'invocation sont disponibles lorsque la charge utile est complète. La taille de la charge utile maximale est de 6 Mo.
- `RESPONSE_STREAM` : permet à votre fonction de diffuser les résultats de la charge utile au fur et à mesure qu'ils sont disponibles. Lambda invoque votre fonction en utilisant l'opération d'API `InvokeWithResponseStream`. La taille maximale de la charge utile de réponse est de 200 Mo.

Vous pouvez toujours invoquer votre fonction sans streaming de réponses en appelant directement l'opération d'API `Invoke`. Cependant, Lambda diffuse toutes les charges utiles de réponse pour les invocations qui passent par l'URL de la fonction jusqu'à ce que vous changiez le mode d'invocation en `BUFFERED`.

Console

Pour définir le mode d'invocation d'une URL de la fonction (console)

1. Ouvrez la page Event Functions de la console Lambda.
2. Sélectionnez le nom de la fonction pour laquelle vous voulez définir le mode d'invocation.
3. Choisissez l'onglet Configuration, puis Function URL (URL de fonction).
4. Sélectionnez Modifier, puis Paramètres supplémentaires.
5. Sous Mode d'invocation, sélectionnez le mode d'invocation de votre choix.
6. Cliquez sur Enregistrer.

AWS CLI

Pour définir le mode d'invocation d'une URL de fonction (AWS CLI)

```
aws lambda update-function-url-config \
  --function-name my-function \
  --invoke-mode RESPONSE_STREAM
```

CloudFormation

Pour définir le mode d'invocation d'une URL de fonction (CloudFormation)

```
MyFunctionUrl:
  Type: AWS::Lambda::Url
  Properties:
    AuthType: AWS_IAM
    InvokeMode: RESPONSE_STREAM
```

Pour de plus amples informations sur la configuration des URL de fonctions, consultez URL de fonctions Lambda.

Tutoriel : création d'une fonction Lambda de streaming de réponses avec une URL de la fonction

Dans ce didacticiel, vous créez une fonction Lambda définie comme archive de fichier ZIP avec un point de terminaison d'URL de la fonction qui renvoie un flux de réponses. Pour de plus amples informations sur la configuration des URL de fonctions, consultez URL de fonctions.

Conditions préalables

Ce didacticiel suppose que vous avez quelques connaissances des opérations Lambda de base et de la console Lambda. Si ce n'est déjà fait, suivez les instructions fournies dans Créer une fonction Lambda à l'aide de la console pour créer votre première fonction Lambda.

Pour effectuer les étapes suivantes, vous avez besoin de l'AWS CLI version 2. Les commandes et la sortie attendue sont répertoriées dans des blocs distincts :

```
aws --version
```

Vous devriez voir la sortie suivante:

```
aws-cli/2.13.27 Python/3.11.6 Linux/4.14.328-248.540.amzn2.x86_64 exe/x86_64.amzn.2
```

Pour les commandes longues, un caractère d'échappement (\) est utilisé pour les fractionner en plusieurs lignes.

Sur Linux et macOS, utilisez votre gestionnaire de shell et de package préféré.

> **Note**
>
> Sous Windows, certaines commandes CLI Bash que vous utilisez couramment avec Lambda (par exemple `zip`) ne sont pas prises en charge par les terminaux intégrés du système d'exploitation. Pour obtenir une Windows-integrated version d'Ubuntu et de Bash, installez le sous-système Windows pour Linux. Les exemples de commandes CLI de ce guide utilisent le formatage Linux. Les commandes qui incluent des documents JSON en ligne doivent être reformatées si vous utilisez la CLI Windows.

Créer un rôle d'exécution

Créez le rôle d'exécution qui donne à votre fonction Lambda l'autorisation d'accéder aux ressources AWS .

Pour créer un rôle d'exécution

1. Accédez à la page Roles (Rôles) de la Gestion des identités et des accès AWS console (IAM).
2. Sélectionnez Créer un rôle.
3. Créez un rôle avec les propriétés suivantes :
   - Type d'entité sécurisée – Service AWS
   - Cas d'utilisation – Lambda
   - Permissions (Autorisations – AWSLambdaBasicExecutionRole
   - Nom de rôle – **`response-streaming-role`**

La AWSLambdaBasicExecutionRolepolitique dispose des autorisations dont la fonction a besoin pour écrire des CloudWatch journaux sur Amazon Logs. Après avoir créé le rôle, notez son Amazon Resource Name (ARN). Vous en aurez besoin à l'étape suivante.

Créez une fonction de diffusion des réponses (AWS CLI)

Créez une fonction Lambda de streaming de réponses avec un point de terminaison d'URL de la fonction à l'aide de l' AWS Command Line Interface (AWS CLI).

Pour créer une fonction capable de diffuser des réponses

1. Copiez l'exemple de code suivant dans un fichier nommé `index.js`. Cette fonction diffuse trois réponses, séparées de 1 seconde.

```
exports.handler = awslambda.streamifyResponse(
 async (event, responseStream, _context) => {
  // Metadata is a JSON serializable JS object. Its shape is not defined here.
  const metadata = {
  statusCode: 200,
  headers: {
   "Content-Type": "application/json",
   "CustomHeader": "outerspace"
  }
  };

  // Assign to the responseStream parameter to prevent accidental reuse of the non-
wrapped stream.
  responseStream = awslambda.HttpResponseStream.from(responseStream, metadata);

  responseStream.write("Streaming with Helper \n");
  await new Promise(r => setTimeout(r, 1000));
  responseStream.write("Hello 0 \n");
  await new Promise(r => setTimeout(r, 1000));
  responseStream.write("Hello 1 \n");
  await new Promise(r => setTimeout(r, 1000));
  responseStream.write("Hello 2 \n");
  await new Promise(r => setTimeout(r, 1000));
  responseStream.end();
  await responseStream.finished();
 }
  );
```

2. Créez un package de déploiement.

```
zip function.zip index.js
```

3. Créez une fonction Lambda à l'aide de la commande `create-function`. Remplacez la valeur de `--role` par l'ARN de rôle de l'étape précédente. Cette commande définit le délai d'expiration de la fonction à 10 secondes, ce qui permet à la fonction de diffuser trois réponses.

```
aws lambda create-function \
  --function-name my-streaming-function \
  --runtime nodejs24.x \
  --zip-file fileb://function.zip \
  --handler index.handler \
  --timeout 10 \
  --role arn:aws:iam::123456789012:role/response-streaming-role
```

Pour créer une URL de la fonction

1. Ajoutez une stratégie basée sur les ressources à votre fonction en accordant les autorisations `lambda:InvokeFunctionUrl` et `lambda:InvokeFunction`. Chaque instruction doit être ajoutée dans une commande distincte. Remplacez la valeur de `--principal` par votre Compte AWS identifiant.

```
aws lambda add-permission \
  --function-name my-streaming-function \
  --action lambda:InvokeFunctionUrl \
  --statement-id UrlPolicyInvokeURL \
  --principal 123456789012 \
  --function-url-auth-type AWS_IAM
```

```
aws lambda add-permission \
    --function-name my-streaming-function \
    --action lambda:InvokeFunction \
    --statement-id UrlPolicyInvokeFunction \
    --principal 123456789012
```

2. Créez un point de terminaison d'URL pour la fonction avec la commande `create-function-url-config`.

```
aws lambda create-function-url-config \
  --function-name my-streaming-function \
  --auth-type AWS_IAM \
  --invoke-mode RESPONSE_STREAM
```

> **Note**
>
> Si un message d'erreur concernant `--invoke-mode` s'affiche, il se peut que vous deviez effectuer une mise à niveau vers une version plus récente d' AWS CLI.

Test du point de terminaison d'URL de fonction

Testez votre intégration en invoquant votre fonction. Vous pouvez ouvrir l'URL de votre fonction dans un navigateur ou utiliser curl.

```
curl --request GET "https://abcdefghijklm7nop7qrs740abcd.lambda-url.us-east-1.on.aws/"
 --user "AKIAIOSFODNN7EXAMPLE" --aws-sigv4 "aws:amz:us-east-1:lambda" --no-buffer
```

Notre URL de la fonction utilise le type d'authentification `IAM_AUTH`. Cela signifie que vous devez signer les demandes à la fois avec votre clé d'accès AWS et votre clé secrète. Dans la commande précédente, remplacez par `AKIAIOSFODNN7EXAMPLE` l'ID de la clé d' AWS accès. Entrez votre clé AWS secrète lorsque vous y êtes invité. Si vous n'avez pas votre clé AWS secrète, vous pouvez utiliser des AWS informations d'identification temporaires à la place.

Vous devriez obtenir une réponse comme celle-ci :

```
Streaming with Helper
Hello 0
Hello 1
Hello 2
```

Nettoyage de vos ressources

Vous pouvez maintenant supprimer les ressources que vous avez créées pour ce didacticiel, sauf si vous souhaitez les conserver. En supprimant AWS les ressources que vous n'utilisez plus, vous évitez des frais inutiles pour votre Compte AWS.

Pour supprimer le rôle d'exécution

1. Ouvrez la page Roles (Rôles) de la console IAM.
2. Sélectionnez le rôle d'exécution que vous avez créé.
3. Sélectionnez Supprimer.

4. Saisissez le nom du rôle dans le champ de saisie de texte et choisissez Delete (Supprimer).

Pour supprimer la fonction d'événement Lambda

1. Ouvrez la page Event Functions de la console Lambda.
2. Sélectionnez la fonction d'événement que vous avez créée.
3. Sélectionnez Actions, Supprimer.
4. Saisissez **`confirm`** dans la zone de saisie de texte et choisissez Delete (Supprimer).

Utilisation du point de terminaison de métadonnées Lambda

Avec le point de terminaison de métadonnées Lambda, vos fonctions peuvent découvrir dans quelle zone de disponibilité (AZ) elles s'exécutent. Vous pouvez l'utiliser pour optimiser la latence en acheminant vers des ressources de même zone de zone de disponibilité, telles que les points de terminaison ElastiCache Amazon et Amazon RDS, et pour implémenter des modèles de résilience. AZ-aware

Le point de terminaison renvoie les métadonnées dans un format JSON simple via une API HTTP localhost au sein de l'environnement d'exécution et est accessible à la fois aux environnements d'exécution et aux extensions.

Sections

- Prise en main
- Comprendre les identifiants des zones de disponibilité
- Référence des API

Prise en main

Powertools for AWS Lambda fournit un utilitaire permettant d'accéder au point de terminaison des métadonnées Lambda en Python TypeScript, Java et .NET. L'utilitaire met en cache la réponse après le premier appel et gère automatiquement l'invalidation SnapStart du cache.

Utilisez l'utilitaire de métadonnées Powertools for AWS Lambda ou appelez directement le point de terminaison des métadonnées

Python

Installez le package Powertools :

```
pip install "aws-lambda-powertools"
```

Utilisez l'utilitaire de métadonnées de votre gestionnaire :

Example Récupération d'un identifiant AZ avec Powertools (Python)

```
from aws_lambda_powertools.utilities.lambda_metadata import get_lambda_metadata
```

```
def handler(event, context):
    metadata = get_lambda_metadata()
    az_id = metadata.availability_zone_id  # e.g., "use1-az1"

    return {"az_id": az_id}
```

TypeScript

Installez le package Powertools :

```
npm install @aws-lambda-powertools/commons
```

Utilisez l'utilitaire de métadonnées de votre gestionnaire :

Example Récupération d'un identifiant AZ avec Powertools () TypeScript

```
import { getMetadata } from '@aws-lambda-powertools/commons/utils/metadata';

const metadata = await getMetadata();

export const handler = async () => {
  const { AvailabilityZoneID: azId } = metadata;
  return azId;
};
```

Java

Ajoutez la dépendance Powertools à votre `pom.xml` :

```
<dependencies>
    <dependency>
        <groupId>software.amazon.lambda</groupId>
        <artifactId>powertools-lambda-metadata</artifactId>
        <version>2.10.0</version>
    </dependency>
</dependencies>
```

Utilisez le client de métadonnées dans votre gestionnaire :

Example Récupération d'un identifiant AZ avec Powertools (Java)

```
import software.amazon.lambda.powertools.metadata.LambdaMetadata;
import software.amazon.lambda.powertools.metadata.LambdaMetadataClient;

public class App implements RequestHandler<Object, String> {

    @Override
    public String handleRequest(Object input, Context context) {
        LambdaMetadata metadata = LambdaMetadataClient.get();
        String azId = metadata.getAvailabilityZoneId(); // e.g., "use1-az1"

        return "{\"azId\": \"" + azId + "\"}";
    }
}
```

.NET

Installez le package Powertools :

```
dotnet add package AWS.Lambda.Powertools.Metadata
```

Utilisez la classe de métadonnées dans votre gestionnaire :

Example Récupération d'un identifiant AZ avec Powertools (.NET)

```
using AWS.Lambda.Powertools.Metadata;

public class Function
{
    public string Handler(object input, ILambdaContext context)
    {
        var azId = LambdaMetadata.AvailabilityZoneId;
        return $"Running in AZ: {azId}";
    }
}
```

All Runtimes

Tous les environnements d'exécution Lambda prennent en charge le point de terminaison des métadonnées, y compris les environnements d'exécution personnalisés et les images de conteneur. Utilisez l'exemple suivant pour accéder à l'API de métadonnées directement depuis

votre fonction à l'aide des variables d'environnement que Lambda définit automatiquement dans l'environnement d'exécution.

Example Accès direct au point de terminaison des métadonnées

```
# Variables are automatically set by Lambda
METADATA_ENDPOINT="http://${AWS_LAMBDA_METADATA_API}/2026-01-15/metadata/execution-
environment"

# Make the request
RESPONSE=$(curl -s -H "Authorization: Bearer ${AWS_LAMBDA_METADATA_TOKEN}"
 "$METADATA_ENDPOINT")

# Parse the AZ ID
AZ_ID=$(echo "$RESPONSE" | jq -r '.AvailabilityZoneID')

echo "Function is running in AZ ID: $AZ_ID"
```

Comprendre les identifiants des zones de disponibilité

Les identifiants AZ (par exemple`use1-az1`) font toujours référence au même emplacement physique sur tous les AWS comptes, tandis que les noms AZ (par exemple`us-east-1a`) peuvent correspondre à une infrastructure physique différente dans chaque AWS compte dans certaines régions. Pour plus d'informations, consultez la section AZ IDs pour la cohérence entre comptes.

Conversion d'un ID AZ en nom AZ :

Pour convertir un ID AZ en nom AZ, utilisez l'API Amazon EC2. DescribeAvailabilityZones Pour utiliser cette API, ajoutez l'`ec2:DescribeAvailabilityZones`autorisation au rôle d'exécution de votre fonction.

Référence des API

Variables d’environnement

Lambda définit automatiquement les variables d'environnement suivantes dans chaque environnement d'exécution :

- `AWS_LAMBDA_METADATA_API`— L'adresse du serveur de métadonnées au format `{ipv4_address}:{port}` (par exemple,`169.254.100.1:9001`).

- `AWS_LAMBDA_METADATA_TOKEN`— Un jeton d'authentification unique pour l'environnement d'exécution actuel. Lambda génère ce jeton automatiquement lors de l'initialisation. Incluez-le dans toutes les demandes d'API de métadonnées.

Endpoint

`GET http://${AWS_LAMBDA_METADATA_API}/2026-01-15/metadata/execution-environment`

Demande

En-têtes obligatoires :

- `Authorization`— La valeur du jeton de la variable d'`AWS_LAMBDA_METADATA_TOKEN`environnement avec le schéma Bearer :`Bearer <token>`. Cette authentification basée sur des jetons fournit une protection approfondie contre les vulnérabilités liées à la falsification des Server-Side requêtes (SSRF). Chaque environnement d'exécution reçoit un jeton unique généré aléatoirement lors de l'initialisation.

Réponse

État : `200 OK`

Content-Type: `application/json`

Cache-Control: `private, max-age=43200, immutable`

La réponse est immuable dans un environnement d'exécution. Les clients doivent mettre en cache la réponse et respecter le `Cache-Control` TTL. Pour les SnapStart fonctions, le TTL est réduit lors de l'initialisation afin que les clients actualisent les métadonnées après la restauration lorsque l'environnement d'exécution peut se trouver dans une autre zone de disponibilité. Si vous utilisez Powertools, la mise en cache et l' SnapStart invalidation sont gérées automatiquement.

Corps de texte:

```
{
  "AvailabilityZoneID": "use1-az1"
}
```

Le `AvailabilityZoneID` champ contient l'identifiant unique de la zone de disponibilité dans laquelle s'exécute l'environnement d'exécution.

> **Note**
>
> Des champs supplémentaires pourraient être ajoutés à la réponse lors de futures mises à jour. Les clients doivent ignorer les champs inconnus et ne pas échouer si de nouveaux champs apparaissent.

Réponses d'erreur

- 401 Non autorisé — L'`Authorization`en-tête est manquant ou contient un jeton non valide. Vérifiez que vous êtes en train de réussir`Bearer ${AWS_LAMBDA_METADATA_TOKEN}`.
- 405 Méthode non autorisée — La méthode de demande ne l'est pas`GET`.
- 500 Erreur interne du serveur — erreur Server-side de traitement.

Comprendre les méthodes d'appel de la fonction d'événement Lambda

Après avoir déployé votre fonction d'événement Lambda, vous pouvez l'invoquer de plusieurs manières :

- La console Lambda : utilisez la console Lambda pour créer rapidement un événement de test pour invoquer votre fonction.
- Le AWS SDK — Utilisez le AWS SDK pour appeler votre fonction par programmation.
- L'API Invoke : utilisez l'API Lambda Invoke pour invoquer directement votre fonction.
- The AWS Command Line Interface (AWS CLI) — Utilisez la `aws lambda invoke` AWS CLI commande pour appeler directement votre fonction depuis la ligne de commande.
- Un point de terminaison HTTP(S) d'URL de la fonction : utilisez des URL de fonctions pour créer un point de terminaison HTTP(S) dédié que vous pouvez utiliser pour invoquer votre fonction.

Toutes ces méthodes sont des moyens directs d'invoquer votre fonction d'événement. Dans Lambda, un cas d'utilisation courant consiste à invoquer votre fonction en fonction d'un événement qui se

produit ailleurs dans votre application. Certains services peuvent invoquer une fonction d'événement Lambda à chaque nouvel événement.

C'est ce qu'on appelle un déclencheur. Pour les services basés sur les flux et les files d'attente, Lambda invoque la fonction avec des lots d'enregistrements. C'est ce qu'on appelle un mappage des sources d'événements.

Lorsque vous invoquez une fonction d'événement, vous pouvez choisir de l'appeler de manière synchrone ou asynchrone. Avec une invocation synchrone, vous attendez de la fonction qu'elle traite l'événement et renvoie une réponse. Avec l'invocation asynchrone, Lambda place en file d'attente l'événement à traiter, et renvoie une réponse immédiatement. Le paramètre de requête `InvocationType` de l'API Invoke détermine la manière dont Lambda appelle votre fonction. Une valeur `RequestResponse` indique une invocation synchrone et une valeur `Event` indique une invocation asynchrone.

Pour appeler votre fonction d'événement via IPv6, utilisez les points de terminaison publics à double pile de Lambda. Dual-stack les points de terminaison prennent en charge à la fois les protocoles IPv4 et IPv6. Les points de terminaison à double pile de Lambda utilisent la syntaxe suivante :

```
protocol://lambda.us-east-1.api.aws
```

Vous pouvez également utiliser les URL de fonctions Lambda pour invoquer des fonctions sur IPv6. Les points de terminaison URL de fonction ont le format suivant :

```
https://url-id.lambda-url.us-east-1.on.aws
```

Si l'invocation de la fonction d'événement entraîne une erreur, pour les invocations synchrones, consultez le message d'erreur dans la réponse et réessayez l'appel manuellement. Pour les invocations asynchrones, Lambda gère les nouvelles tentatives et peut envoyer des enregistrements d'invocation à une destination.

Invoquer une fonction d'événement Lambda de manière synchrone

Lorsque vous appelez une fonction d'événement Lambda de manière synchrone, Lambda exécute la fonction et attend une réponse. Une fois l'exécution de la fonction terminée, Lambda renvoie la réponse du code de la fonction avec des données supplémentaires, telles que la version de la fonction qui a été invoquée. Pour appeler une fonction de manière synchrone avec le AWS CLI, utilisez la `invoke` commande.

```
aws lambda invoke --function-name my-function \
    --cli-binary-format raw-in-base64-out \
    --payload '{ "key": "value" }' response.json
```

L'cli-binary-formatoption est obligatoire si vous utilisez AWS CLI la version 2. Pour faire de ce paramètre le paramètre par défaut, exécutez `aws configure set cli-binary-format raw-in-base64-out`. Pour plus d'informations, consultez les options de ligne de commande globales AWS CLI prises en charge dans le Guide de l'utilisateur AWS Command Line Interface version 2.

Vous devriez voir la sortie suivante :

```
{
    "ExecutedVersion": "$LATEST",
    "StatusCode": 200
}
```

Le schéma suivant montre les clients qui invoquent une fonction d'événement Lambda de manière synchrone. Lambda envoie les événements directement à la fonction et renvoie la réponse de la fonction à l'appelant.

`payload` est une chaîne qui contient un événement au format JSON. Le nom du fichier où l' AWS CLI écrit la réponse de la fonction est `response.json`. Si la fonction d'événement renvoie un objet ou une erreur, le corps de la réponse est l'objet ou l'erreur au format JSON. Si la fonction se termine sans erreur, le corps de la réponse est `null`.

> **Note**
>
> Lambda n'attend pas que les extensions externes se terminent avant d'envoyer la réponse. Les extensions externes s'exécutent comme des processus indépendants dans l'environnement d'exécution et continuent de s'exécuter après l'invocation de la fonction. Pour plus d'informations, consultez Améliorez les fonctions d'événement Lambda à l'aide des extensions Lambda.

La sortie de la commande qui s'affiche dans le terminal inclut des informations extraites d'en-têtes figurant dans la réponse de Lambda. Ces informations incluent la version qui a traité l'événement (utile lorsque vous utilisez des alias) et le code d'état renvoyé par Lambda. Si Lambda a pu exécuter la fonction, le code d'état est 200, même si la fonction a renvoyé une erreur.

> **Note**
>
> Pour les fonctions événementielles dont le délai d'expiration est long, votre client peut être déconnecté lors d'un appel synchrone pendant qu'il attend une réponse. Configurez votre client HTTP, SDK, pare-feu, proxy ou système d'exploitation pour permettre des connexions longues avec des paramètres de délai d'attente ou de keep-alive.

Si Lambda ne parvient pas à exécuter la fonction d'événement, l'erreur s'affiche dans la sortie.

```
aws lambda invoke --function-name my-function \
    --cli-binary-format raw-in-base64-out \
    --payload value response.json
```

Vous devriez voir la sortie suivante :

```
An error occurred (InvalidRequestContentException) when calling the Invoke operation:
 Could not parse request body into json: Unrecognized token 'value': was expecting
 ('true', 'false' or 'null')
```

```
 at [Source: (byte[])"value"; line: 1, column: 11]
```

AWS CLI Il s'agit d'un outil open source que vous pouvez utiliser pour interagir avec les AWS services à l'aide de commandes dans votre interface de ligne de commande. Pour effectuer les étapes de cette section, vous devez disposer de la version 2 de l'AWS CLI.

Vous pouvez utiliser AWS CLI pour récupérer les journaux d'une invocation à l'aide de l'option de commande `--log-type`. La réponse inclut un champ `LogResult` qui contient jusqu'à 4 Ko de journaux codés en base64 provenant de l'invocation.

Example récupérer un ID de journal

L'exemple suivant montre comment récupérer un ID de journal à partir du champ `LogResult` d'une fonction nommée `my-function`.

```
aws lambda invoke --function-name my-function out --log-type Tail
```

Vous devriez voir la sortie suivante:

```
{
    "StatusCode": 200,
    "LogResult":
 "U1RBUlQgUmVxdWVzdElkOiA4N2QwNDRiOC1mMTU0LTExZTgtOGNkYS0yOTc0YzVlNGZiMjEgVmVyc2lvb...",
    "ExecutedVersion": "$LATEST"
}
```

Example décoder les journaux

Dans la même invite de commandes, utilisez l'utilitaire `base64` pour décoder les journaux. L'exemple suivant montre comment récupérer les journaux encodés en base64 pour `my-function`.

```
aws lambda invoke --function-name my-function out --log-type Tail \
--query 'LogResult' --output text --cli-binary-format raw-in-base64-out | base64 --
decode
```

L'cli-binary-formatoption est obligatoire si vous utilisez AWS CLI la version 2. Pour faire de ce paramètre le paramètre par défaut, exécutez `aws configure set cli-binary-format raw-in-base64-out`. Pour plus d'informations, consultez les options de ligne de commande globales AWS CLI prises en charge dans le Guide de l'utilisateur AWS Command Line Interface version 2.

Vous devriez voir la sortie suivante :

```
START RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8 Version: $LATEST
"AWS_SESSION_TOKEN": "AgoJb3JpZ2luX2VjELj...", "_X_AMZN_TRACE_ID": "Root=1-5d02e5ca-
f5792818b6fe8368e5b51d50;Parent=191db58857df8395;Sampled=0"",ask/lib:/opt/lib",
END RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8
REPORT RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8  Duration: 79.67 ms      Billed
 Duration: 80 ms         Memory Size: 128 MB     Max Memory Used: 73 MB
```

L'utilitaire `base64` est disponible sous Linux, macOS et Ubuntu sous Windows. Les utilisateurs de macOS auront peut-être besoin d'utiliser `base64 -D`.

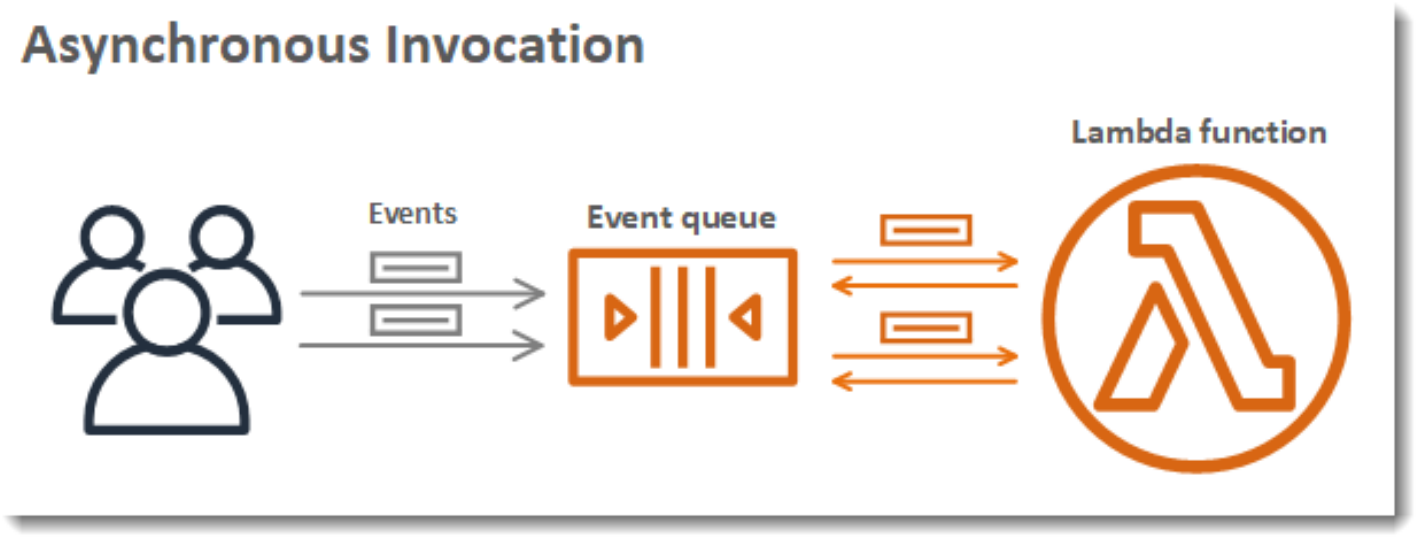
Pour plus d'informations sur l'API `Invoke` et la liste complète des paramètres, en-têtes et erreurs, consultez Invoquer.

Lorsque vous invoquez directement une fonction d'événement, vous pouvez vérifier la présence d'erreurs dans la réponse et réessayer. Le AWS SDK AWS CLI et le SDK réessayent également automatiquement en cas d'expiration du délai d'expiration, de limitation et d'erreur de service du client. Pour plus d'informations, consultez Comprendre le comportement des nouvelles tentatives dans les fonctions d'événement Lambda.

Invocation d'une fonction d'événement Lambda de manière asynchrone

Plusieurs d' Services AWS entre eux, tels qu'Amazon Simple Storage Service (Amazon S3) et Amazon Simple Notification Service (Amazon SNS), invoquent des fonctions d'événement de manière asynchrone pour traiter les événements. Vous pouvez également appeler une fonction d'événement Lambda de manière asynchrone à l'aide du AWS Command Line Interface (AWS CLI) ou de l'un des SDK. AWS Lorsque vous appelez une fonction d'événement de manière asynchrone, vous n'attendez pas de réponse du code de la fonction. Vous remettez l'événement à Lambda qui se charge du reste. Vous pouvez configurer la manière dont Lambda gère les erreurs et envoyer des enregistrements d'invocation à une ressource en aval telle qu'Amazon Simple Queue Service (Amazon SQS) ou EventBridge EventBridge Amazon () pour enchaîner les composants de votre application.

Le diagramme suivant montre des clients invoquant une fonction Lambda de manière asynchrone. Lambda place les événements en file d'attente avant de les envoyer à la fonction.



Pour une invocation asynchrone, Lambda place l'événement dans une file d'attente et renvoie une réponse de succès sans plus informations. Un processus distinct lit les événements à partir de la file d'attente et les envoie à votre fonction.

Pour appeler une fonction d'événement Lambda de manière asynchrone à l'aide du AWS Command Line Interface (AWS CLI) ou de l'un des AWS SDK, définissez le paramètre sur. [InvocationType](#)`Event` L'exemple suivant montre une AWS CLI commande pour appeler une fonction.

```
aws lambda invoke \
  --function-name my-function  \
```

```
  --invocation-type Event \
  --cli-binary-format raw-in-base64-out \
  --payload '{ "key": "value" }' response.json
```

Vous devriez voir la sortie suivante :

```
{
    "StatusCode": 202
}
```

L'cli-binary-formatoption est obligatoire si vous utilisez AWS CLI la version 2. Pour faire de ce paramètre le paramètre par défaut, exécutez `aws configure set cli-binary-format raw-in-base64-out`. Pour plus d'informations, consultez les options de ligne de commande globales prises en charge par l'AWS CLI dans le Guide de l'utilisateur AWS Command Line Interface version 2.

Le fichier de sortie (`response.json`) ne contient pas d'informations, mais il est tout de même créé lorsque vous exécutez cette commande. Si Lambda n'est pas en mesure d'ajouter l'événement à la file d'attente, un message d'erreur s'affiche dans la sortie de la commande.

Méthode de gestion des erreurs et nouvelles tentatives d'invocation asynchrone par Lambda

Lambda gère la file d'attente d'événements asynchrones de votre fonction, et effectue de nouvelles tentatives en cas d'erreur. Si la fonction renvoie une erreur, Lambda tente par défaut de l'exécuter deux fois de plus, avec une minute d'attente entre les deux premières tentatives, et deux minutes entre la deuxième et la troisième tentative. Les erreurs liées à la fonction événementielle incluent les erreurs renvoyées par le code de la fonction et les erreurs renvoyées par l'exécution de la fonction, telles que les délais d'attente.

Si la fonction d'événement ne dispose pas d'une simultanéité suffisante pour traiter tous les événements, les demandes supplémentaires sont limitées. Pour les erreurs de limitation (429) et les erreurs système (série 500), Lambda renvoie l'événement dans la file d'attente et tente d'exécuter à nouveau la fonction pendant une période pouvant aller jusqu'à 6 heures par défaut. L'intervalle de nouvelle tentative augmente de manière exponentielle de 1 seconde après la première tentative jusqu'à un maximum de 5 minutes. Si la file d'attente contient de nombreuses entrées, Lambda augmente l'intervalle entre les tentatives et réduit la fréquence des événements de lecture à partir de la file d'attente.

Même si votre fonction d'événement ne renvoie pas d'erreur, il est possible qu'elle reçoive le même événement de Lambda plusieurs fois, car la file d'attente elle-même est finalement cohérente. Si la fonction ne peut pas à prendre en charge les événements entrants, ils peuvent également être supprimés de la file d'attente sans être envoyés à la fonction. Assurez-vous que le code de votre fonction gère correctement les événements dupliqués et que vous avez suffisamment de simultanéité disponible pour gérer toutes les invocations.

Lorsque la file d'attente est très longue, les nouveaux événements peuvent vieillir avant que Lambda n'ait l'occasion de les envoyer à votre fonction d'événement. Quand un événement expire ou échoue à toutes les tentatives de traitement, Lambda le supprime. Vous pouvez configurer la gestion des erreurs pour une fonction d'événement afin de réduire le nombre de tentatives effectuées par Lambda ou de supprimer plus rapidement les événements non traités. Pour capturer les événements supprimés, configurez une file d'attente de lettres mortes pour la fonction. Pour capturer les enregistrements des invocations ayant échoué (comme les expirations de délai d'expiration ou les erreurs d'environnement d'exécution), créez une destination en cas d'échec.

Configuration de la gestion des erreurs pour les invocations asynchrones Lambda

Utilisez les paramètres suivants pour configurer la façon dont Lambda gère les erreurs et les nouvelles tentatives pour les invocations de fonctions asynchrones :

- MaximumEventAgeInSeconds: durée maximale, en secondes, pendant laquelle Lambda conserve un événement dans la file d'attente d'événements asynchrones avant de le supprimer.
- MaximumRetryAttempts: le nombre maximum de fois que Lambda réessaie des événements lorsque la fonction renvoie une erreur.

Utilisez la console Lambda ou AWS CLI pour configurer les paramètres de gestion des erreurs sur une fonction d'événement, une version ou un alias.

Console

Pour configurer la gestion des erreurs

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez une fonction d'événement.
3. Sélectionnez Configuration, puis Asynchronous invocation (Invocation asynchrone).
4. Sous Asynchronous invocation (Invocation asynchrone), choisissez Edit (Modifier).
5. Configurez les paramètres suivants.

- Maximum age of event (Âge maximal de l'événement) – Durée maximale, jusqu'à 6 heures, pendant laquelle Lambda conserve un événement dans la file d'attente d'événements asynchrones.
- Retry attempts (Nouvelles tentatives) – Nombre de nouvelles tentatives, entre 0 et 2, que Lambda effectue lorsque la fonction renvoie une erreur.

6. Cliquez sur Enregistrer.

AWS CLI

Pour configurer l'invocation asynchrone avec le, utilisez la commande AWS CLI put-function-event-invoke-config. L'exemple suivant configure une fonction d'événement avec une durée maximale d'un événement d'une heure et aucune nouvelle tentative.

```
aws lambda put-function-event-invoke-config \
  --function-name error \
  --maximum-event-age-in-seconds 3600 \
  --maximum-retry-attempts 0
```

La commande `put-function-event-invoke-config` remplace toute configuration existante sur la fonction, la version ou l'alias. Pour configurer une option sans en réinitialiser d'autres, utilisez update-function-event-invoke-config. L'exemple suivant illustre la configuration de Lambda pour l'envoie d'un enregistrement à une file d'attente SQS standard nommée `destination` lorsqu'un événement ne peut pas être traité.

```
aws lambda update-function-event-invoke-config \
  --function-name my-function \
  --destination-config '{"OnFailure":{"Destination": "arn:aws:sqs:us-
east-1:123456789012:destination"}}'
```

Vous devriez voir la sortie suivante :

```
{
    "LastModified": 1573686021.479,
    "FunctionArn": "arn:aws:lambda:us-east-1:123456789012:function:my-function:
$LATEST",
    "MaximumRetryAttempts": 0,
    "MaximumEventAgeInSeconds": 3600,
```

```
    "DestinationConfig": {
        "OnSuccess": {},
        "OnFailure": {}
    }
}
```

Quand un événement d'invocation dépasse l'âge maximum ou échoue à toutes les tentatives, Lambda le supprime. Pour conserver une copie des événements supprimés, configurez une destination pour les événements ayant échoué.

Capture des enregistrements d'invocations asynchrones Lambda

Lambda peut envoyer des enregistrements d'appels asynchrones à l'une des entités suivantes. Services AWS

- Amazon SQS : une file d'attente SQS standard
- Amazon SNS : une rubrique SNS standard
- Amazon S3 : un compartiment Amazon S3 (uniquement en cas d'échec)
- AWS Lambda : une fonction Lambda
- Amazon EventBridge — Un bus EventBridge événementiel

L'enregistrement d'invocation contient des détails sur la demande et la réponse au format JSON. Vous pouvez configurer des destinations distinctes pour les événements qui ont été traités avec succès et ceux dont le traitement a échoué. Vous pouvez également configurer une file d'attente Amazon SQS ou une rubrique Amazon SNS standard en tant que file d'attente de lettres mortes pour les événements abandonnés. Pour les files d'attente de lettres mortes, Lambda envoie uniquement le contenu de l'événement, sans plus d'informations sur la réponse.

Si Lambda ne parvient pas à envoyer un enregistrement vers une destination que vous avez configurée, il envoie une `DestinationDeliveryFailures` métrique à Amazon. CloudWatch Cela peut se produire si votre configuration inclut un type de destination non pris en charge, tel qu'une file d'attente FIFO Amazon SQS ou une rubrique FIFO Amazon SNS. Des erreurs de remise peuvent également se produire en raison d'erreurs d'autorisations et de limites de taille. Pour plus d'informations sur les métriques d'invocation Lambda, consultez the section called “Métriques d'invocation”.

> **Note**
>
> Pour empêcher le déclenchement d'une fonction événementielle, vous pouvez définir la simultanéité réservée de la fonction sur zéro. Lorsque vous définissez la simultanéité réservée sur zéro pour une fonction invoquée de manière asynchrone, Lambda commence à envoyer les nouveaux événements à la file d'attente de lettres mortes ou à la destination d'événement en situation d'échec, sans aucune nouvelle tentative. Pour traiter les événements qui ont été envoyés alors que la simultanéité réservée était définie sur zéro, vous devez consommer les événements de la file d'attente de lettres mortes ou de la destination des événements en situation d'échec.

Ajout d'une destination

Pour conserver les enregistrements des appels asynchrones, ajoutez une destination à votre fonction d'événement. Vous pouvez choisir d'envoyer les invocations réussies ou non à une destination. Chaque fonction peut avoir plusieurs destinations. Vous pouvez donc configurer des destinations distinctes pour les événements réussis et échoués. Chaque enregistrement envoyé à la destination est un document JSON avec des détails sur l'invocation. Tout comme les paramètres de gestion des erreurs, vous pouvez configurer les destinations sur une fonction événementielle, une version de fonction ou un alias.

> **Tip**
>
> Vous pouvez également conserver les enregistrements des appels ayant échoué pour les types de mappage de sources d'événements suivants : Amazon Kinesis, Amazon DynamoDB et Apache Kafka (Amazon MSK et Apache Kafka autogéré).

Le tableau suivant répertorie les destinations prises en charge pour les enregistrements d'invocation asynchrones. Pour que Lambda envoie correctement les enregistrements vers la destination que vous avez choisie, assurez-vous que le rôle d'exécution de votre fonction d'événement contient également les autorisations appropriées. Le tableau décrit également comment chaque type de destination reçoit l'enregistrement d'invocation JSON.

Type de destination	Autorisation obligatoire	Destination-specific Format JSON
File d'attente Amazon SQS	sqs : SendMessage	Lambda transmet l'enregis trement d'invocation en tant que `Message` à la destination.
Rubrique Amazon SNS	sns:Publish	Lambda transmet l'enregis trement d'invocation en tant que `Message` à la destination.
Compartiment Amazon S3 (uniquement en cas d'échec)	s3 : PutObject s3 : ListBucket	• Lambda stocke l'enregis trement d'invocation en tant qu'objet JSON dans le compartiment de destinati on. • Le nom de l'objet S3 utilise la convention de dénominat ion suivante : `aws/lambda/async/<function-name>/YYYY/MM/DD/YYYY-MM-DDTHH.MM.SS-<Random UUID>`
Fonction d'événement Lambda	lambda : InvokeFunction	Lambda transmet l'enregis trement d'invocation comme charge utile à la fonction.
EventBridge	événements : PutEvents	• Lambda transmet l'enregis trement d'invocation tel qu'il figure `detail` dans l'appel. PutEvents • La valeur du champ événement `source` est `lambda`.

Type de destination	Autorisation obligatoire	Destination-specific Format JSON
		• La valeur du champ événement `detail-type` est soit Résultat de l'invocation de la fonction lambda – Succès, soit Résultat de l'invocation de la fonction lambda – Échec. • Le champ d'événement `resource` contient la fonction et les Amazon Resource Names (ARNs) de destination. • Pour les autres champs relatifs aux événements, consultez Amazon EventBridge events.

> **Note**
>
> Pour les destinations Amazon S3, si vous avez activé le chiffrement sur le compartiment à l'aide d'une clé KMS, votre fonction d'événement a également besoin de l'GenerateDataKeyautorisation kms :.

> **Important**
>
> Lorsque vous utilisez Amazon SNS comme destination, sachez que la taille maximale des messages d'Amazon SNS est limitée à 256 Ko. Si votre charge utile d'appel asynchrone approche 1 Mo, l'enregistrement d'appel (qui inclut la charge utile d'origine ainsi que des métadonnées supplémentaires) peut dépasser la limite Amazon SNS et entraîner des échecs de livraison. Envisagez d'utiliser des destinations Amazon SQS ou Amazon S3 pour des données utiles plus importantes.

Les étapes suivantes expliquent comment configurer une destination pour une fonction à l'aide de la console Lambda et de l' AWS CLI.

Console

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez une fonction d'événement.
3. Sous Function overview (Vue d'ensemble de la fonction), choisissez Add destination (Ajouter une destination).
4. Pour Source, choisissez Asynchronous invocation (Invocation asynchrone).
5. Pour Condition choisissez l'une des options suivantes :
   - On failure (En cas d'échec) – Envoyer un enregistrement quand l'événement échoue à toutes les tentatives de traitement ou dépasse l'âge maximal.
   - On success (En cas de succès) – Envoyer un enregistrement quand la fonction traite avec succès une invocation asynchrone.
6. Pour Type de destination, choisissez le type de ressource qui reçoit l'enregistrement d'invocation.
7. Pour Destination, choisissez une ressource.
8. Cliquez sur Enregistrer.

AWS CLI

Pour configurer une destination à l'aide de AWS CLI, exécutez la commande update-function-event-invoke-config. L'exemple suivant illustre la configuration de Lambda pour l'envoie d'un enregistrement à une file d'attente SQS standard nommée `destination` lorsqu'un événement ne peut pas être traité.

```
aws lambda update-function-event-invoke-config \
  --function-name my-function \
  --destination-config '{"OnFailure":{"Destination": "arn:aws:sqs:us-
east-1:123456789012:destination"}}'
```

Pratiques exemplaires en matière de sécurité pour les destinations Amazon S3

La suppression d'un compartiment S3 configuré comme destination sans supprimer la destination de la configuration de votre fonction peut engendrer un risque de sécurité. Si un autre utilisateur connaît le nom de votre compartiment de destination, il peut recréer le compartiment dans son Compte AWS. Les enregistrements des invocations ayant échoué seront envoyés dans son compartiment, exposant potentiellement les données de votre fonction.

> **Warning**
>
> Pour vous assurer que les enregistrements d'invocation de votre fonction d'événement ne peuvent pas être envoyés vers un compartiment S3 d'un autre Compte AWS, ajoutez une condition au rôle d'exécution de votre fonction qui limite `s3:PutObject` les autorisations aux compartiments de votre compte.

L'exemple suivant présente une politique IAM qui limite les autorisations `s3:PutObject` de votre fonction aux seuls compartiments de votre compte. Cette politique donne également à Lambda l'autorisation `s3:ListBucket` dont il a besoin pour utiliser un compartiment S3 comme destination.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3BucketResourceAccountWrite",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::*/*",
                "arn:aws:s3:::*"
            ],
            "Condition": {
                "StringEquals": {
                    "s3:ResourceAccount": "111122223333"
                }
            }
        }
    ]
```

```
}
```

Pour ajouter une politique d'autorisations au rôle d'exécution de votre fonction à l'aide du Console de gestion AWS ou AWS CLI, reportez-vous aux instructions des procédures suivantes :

Console

Pour ajouter une politique d’autorisations au rôle d’exécution d’une fonction (console)

1. Ouvrez la page Event Functions de la console Lambda.
2. Sélectionnez la fonction d'événement Lambda dont vous souhaitez modifier le rôle d'exécution.
3. Sous l’onglet Configuration, sélectionnez Autorisations.
4. Sous l’onglet Rôle d’exécution, sélectionnez le Nom du rôle de votre fonction pour ouvrir la page de console IAM du rôle.
5. Ajoutez une politique d’autorisations de au rôle en procédant comme suit :

    a. Dans le volet Politiques d’autorisations, choisissez Ajouter des autorisations, puis Créer une politique en ligne.
    b. Dans l’Éditeur de politique, sélectionnez JSON.
    c. Collez la politique que vous souhaitez ajouter dans l’éditeur (en remplacement du JSON existant), puis choisissez Suivant.
    d. Sous Détails de la politique, saisissez un Nom de la politique.
    e. Choisissez Create Policy (Créer une politique).

AWS CLI

Pour ajouter une politique d'autorisation au rôle d'exécution (CLI) d'une fonction d'événement

1. Créez un document de politique JSON avec les autorisations requises et enregistrez-le dans un répertoire local.
2. Utilisez la commande `put-role-policy` de la CLI IAM pour ajouter des autorisations au rôle d’exécution de votre fonction. Exécutez la commande suivante depuis le répertoire dans lequel vous avez enregistré votre document de politique JSON et remplacez le nom du rôle, le nom de la politique et le document de politique par vos propres valeurs.

    ```
    aws iam put-role-policy \
    ```

```
--role-name my_lambda_role \
--policy-name LambdaS3DestinationPolicy \
--policy-document file://my_policy.json
```

Exemple d'enregistrement d'invocation

Quand une invocation correspond à la condition, Lambda envoie à la destination un document JSON avec des détails sur l'invocation. L'exemple suivant montre un enregistrement d'appel pour un événement qui a échoué à trois tentatives de traitement en raison d'une erreur de fonction d'événement.

Example

```
{
    "version": "1.0",
    "timestamp": "2019-11-14T18:16:05.568Z",
    "requestContext": {
        "requestId": "e4b46cbf-b738-xmpl-8880-a18cdf61200e",
        "functionArn": "arn:aws:lambda:us-east-1:123456789012:function:my-function:
$LATEST",
        "condition": "RetriesExhausted",
        "approximateInvokeCount": 3
    },
    "requestPayload": {
        "ORDER_IDS": [
            "9e07af03-ce31-4ff3-xmpl-36dce652cb4f",
            "637de236-e7b2-464e-xmpl-baf57f86bb53",
            "a81ddca6-2c35-45c7-xmpl-c3a03a31ed15"
        ]
    },
    "responseContext": {
        "statusCode": 200,
        "executedVersion": "$LATEST",
        "functionError": "Unhandled"
    },
    "responsePayload": {
        "errorMessage": "RequestId: e4b46cbf-b738-xmpl-8880-a18cdf61200e Process exited
 before completing request"
    }
}
```

L’enregistrement d’invocation contient des détails sur l’événement, la réponse et la raison pour laquelle l’enregistrement a été envoyé.

Suivi des demandes vers les destinations

Vous pouvez l'utiliser AWS X-Ray pour voir une vue connectée de chaque demande lorsqu'elle est mise en file d'attente, traitée par une fonction d'événement Lambda et transmise au service de destination. Lorsque vous activez le X-Ray suivi pour une fonction ou un service qui invoque une fonction, Lambda ajoute X-Ray un en-tête à la demande et transmet l'en-tête au service de destination. Les traces des services en amont sont automatiquement liées aux traces des fonctions d'événement Lambda en aval et des services de destination, créant ainsi une vue de bout en bout de l'application dans son intégralité. Pour plus d’informations sur le suivi, consultez Visualisez les invocations de la fonction d'événement Lambda à l'aide de AWS X-Ray.

Ajout d’une file d’attente de lettres mortes

Comme alternative à une destination en cas de défaillance, vous pouvez configurer votre fonction d'événement avec une file d'attente de lettres mortes afin d'enregistrer les événements ignorés pour un traitement ultérieur. Une file d’attente de lettres mortes agit de la même manière qu’une destination réservée aux échecs en ce sens qu’elle est utilisée lorsqu’un événement échoue à toutes les tentatives de traitement ou expire sans être traité. Toutefois, vous ne pouvez ajouter ou supprimer une file d’attente de lettres mortes qu’au niveau de la fonction. Les versions Event Function utilisent les mêmes paramètres de file d'attente de lettres mortes que la version non publiée ($LATEST). On-failure les destinations prennent également en charge des cibles supplémentaires et incluent des détails sur la réponse de la fonction dans l'enregistrement d'appel.

Pour retraiter les événements d'une file d'attente contenant des lettres mortes, vous pouvez la définir comme source d'événements pour votre fonction d'événement Lambda. Vous pouvez également récupérer manuellement les événements.

Vous pouvez choisir une file d’attente Amazon SQS standard ou une rubrique Amazon SNS standanrd pour votre file d’attente de lettres mortes. Les files d’attente FIFO et les rubriques FIFO Amazon SNS ne sont pas prises en charge.

- File d’attente Amazon SQS – Une file d’attente conserve les événements qui ont échoué jusqu’à ce qu’ils soient récupérés. Choisissez une file d'attente standard Amazon SQS si vous vous attendez à ce qu'une seule entité, telle qu'une fonction d'événement Lambda ou une CloudWatch alarme, traite l'événement défaillant. Pour plus d’informations, consultez Utilisation de Lambda avec Amazon SQS.

- Rubrique Amazon SNS – Une rubrique relaie les événements qui ont échoué vers une ou plusieurs destinations. Choisissez une rubrique Amazon SNS standard si vous voulez que plusieurs entités agissent sur un événement ayant échoué. Par exemple, vous pouvez configurer une rubrique pour envoyer des événements à une adresse e-mail, à une fonction d'événement Lambda ou à un point de and/or terminaison HTTP. Pour plus d'informations, consultez Invocation des fonctions d'événement Lambda avec les notifications Amazon SNS.

Pour envoyer des événements vers une file d'attente ou un sujet, votre fonction d'événement a besoin d'autorisations supplémentaires. Ajoutez une stratégie avec les autorisations requises au rôle d'exécution de votre fonction. Si la file d'attente ou le sujet cible est chiffré à l'aide d'une AWS KMS clé gérée par le client, assurez-vous que le rôle d'exécution de votre fonction et la politique basée sur les ressources de la clé contiennent les autorisations appropriées.

Après avoir créé la cible et mis à jour le rôle d'exécution de votre fonction d'événement, ajoutez la file d'attente de lettres mortes à votre fonction. Vous pouvez configurer plusieurs fonctions pour envoyer des événements à la même cible.

Console

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez une fonction d'événement.
3. Sélectionnez Configuration, puis Asynchronous invocation (Invocation asynchrone).
4. Sous Asynchronous invocation (Invocation asynchrone), choisissez Edit (Modifier).
5. Définissez le service de Dead-letter file d'attente sur Amazon SQS ou Amazon SNS.
6. Choisissez la file d'attente ou la rubrique cible.
7. Cliquez sur Enregistrer.

AWS CLI

Pour configurer une file d'attente contenant des lettres mortes avec le AWS CLI, utilisez la commande update-function-configuration.

```
aws lambda update-function-configuration \
  --function-name my-function \
  --dead-letter-config TargetArn=arn:aws:sns:us-east-1:123456789012:my-topic
```

Lambda envoie l'événement à la file d'attente de lettres mortes en l'état, avec des informations supplémentaires dans les attributs. Vous pouvez utiliser ces informations pour identifier l'erreur que la fonction a renvoyée ou établir une corrélation entre l'événement et des journaux ou une trace AWS X-Ray .

Dead-letter attributs des messages de file d'attente

- RequestID (Chaîne) – ID de la demande d'invocation. Les ID de demande apparaissent dans les journaux de la fonction. Vous pouvez également utiliser le X-Ray SDK pour enregistrer l'ID de demande sur un attribut de la trace. Vous pouvez ensuite rechercher des traces par ID de demande dans la X-Ray console.
- ErrorCode(Numéro) — Le code d'état HTTP.
- ErrorMessage(String) — Les 1 premiers Ko du message d'erreur.

Si Lambda ne parvient pas à envoyer de message à la file d'attente contenant des lettres mortes, il supprime l'événement et émet la métrique. DeadLetterErrors Cela peut se produire en raison d'un manque d'autorisations ou si la taille totale du message est supérieure à la limite de la file d'attente cible ou rubrique. Supposons, par exemple, qu'une notification Amazon SNS dont le corps est proche de 1 Mo déclenche une fonction qui génère une erreur. Dans ce cas, le message peut dépasser la taille maximale autorisée dans la file d'attente de lettres mortes en raison des données d'événement ajoutées par Amazon SNS et de attributs ajoutés par Lambda.

Si vous utilisez Amazon SQS comme source d'événements, configurez une file d'attente de lettres mortes sur la file d'attente Amazon SQS elle-même et non sur la fonction d'événement Lambda. Pour plus d'informations, consultez Utilisation de Lambda avec Amazon SQS.

Procédure de traitement par Lambda des enregistrements provenant de sources d'événements basées sur des flux et des files d'attente

Un mappage des sources d'événements est une ressource Lambda qui lit des éléments à partir de services basés sur des flux et des files d'attente et qui invoque une fonction avec des lots d'enregistrements. Dans le cadre d'un mappage des sources d'événements, des ressources appelées sondeurs d'événements interrogent activement les nouveaux messages et invoquent des fonctions. Par défaut, Lambda adapte automatiquement les sondeurs d'événements, mais pour certains types de sources d'événements, vous pouvez utiliser le mode alloué pour contrôler le nombre minimum et maximum de sondeurs d'événements dédiés votre mappage des sources d'événements.

Les services suivants utilisent des mappages de sources d'événements pour appeler les fonctions d'événement Lambda :

- Amazon DocumentDB (compatible avec MongoDB) (Amazon DocumentDB)
- Amazon DynamoDB
- Amazon Kinesis
- Amazon MQ
- Amazon Managed Streaming for Apache Kafka (Amazon MSK)
- Self-managed Apache Kafka
- Amazon Simple Queue Service (Amazon SQS)

> ⚠ Warning
>
> Les mappages des sources d'événements Lambda traitent chaque événement au moins une fois, et le traitement des enregistrements peut être dupliqué. Pour éviter les problèmes potentiels liés à des événements dupliqués, nous vous recommandons vivement de rendre votre code de fonction idempotent. Pour en savoir plus, consultez Comment rendre ma fonction Lambda idempotente dans le Knowledge Center. AWS

Différence entre les mappages de sources d'événements et les déclencheurs directs

Certains Services AWS peuvent appeler directement les fonctions d'événement Lambda à l'aide de déclencheurs. Ces services envoient des événements à Lambda, et la fonction est invoquée aussitôt

que l'événement spécifié se produit. Les déclencheurs sont adaptés aux événements discrets et au traitement en temps réel. Lorsque vous créez un déclencheur à l'aide de la console Lambda, celle-ci interagit avec le AWS service correspondant pour configurer la notification d'événement sur ce service. Le déclencheur est en fait stocké et géré par le service qui génère les événements, et non par Lambda. Voici quelques exemples de services qui utilisent des déclencheurs pour appeler des fonctions d'événement Lambda :

- Amazon Simple Storage Service (Amazon S3) : invoque une fonction lorsqu'un objet est créé, supprimé ou modifié dans un compartiment. Pour plus d'informations, consultez Tutoriel : Utilisation d'un déclencheur Amazon S3 pour appeler une fonction d'événement Lambda.
- Amazon Simple Notification Service (Amazon SNS) : invoque une fonction lorsqu'un message est publié dans une rubrique SNS. Pour plus d'informations, consultez Tutoriel : Utilisation AWS Lambda avec Amazon Simple Notification Service.
- Amazon API Gateway : invoque une fonction lorsqu'une requête d'API est envoyée à un point de terminaison spécifique. Pour plus d'informations, consultez Invocation d'une fonction d'événement Lambda à l'aide d'un point de terminaison Amazon API Gateway.

Les mappages des sources d'événements sont des ressources Lambda créées et gérées au sein du service Lambda. Les mappages des sources d'événements sont conçus pour traiter de gros volumes de données en streaming ou de messages provenant de files d'attente. Le traitement par lots des enregistrements d'un flux ou d'une file d'attente est plus efficace que le traitement individuel des enregistrements.

Comportement de traitement par lots

Par défaut, un mappage de source d'événements regroupe les enregistrements en une seule charge utile que Lambda envoie à votre fonction d'événement. Pour affiner le comportement du traitement par lots, vous pouvez configurer une fenêtre de traitement par lots (MaximumBatchingWindowInSeconds) et une taille de lot (BatchSize). Une fenêtre de traitement par lots représente l'intervalle de temps maximal pour collecter des enregistrements dans une même charge utile. La taille d'un lot est le nombre maximal d'enregistrements dans un même lot. Lambda invoque votre fonction en présence de l'un des trois critères suivants :

- La fenêtre de traitement par lots atteint sa valeur maximale. Le comportement par défaut de la fenêtre de traitement par lots varie selon la source d'événement spécifique.
  - Pour les sources d'événements Kinesis, DynamoDB et Amazon SQS : la fenêtre de traitement par lot par défaut est de 0 seconde. Cela signifie que Lambda invoque votre fonction dès que

des enregistrements sont disponibles. Pour définir une fenêtre de traitement par lots, configurez `MaximumBatchingWindowInSeconds`. Vous pouvez configurer ce paramètre à n'importe quelle valeur comprise entre 0 et 300 secondes par incréments d'1 seconde. Si vous configurez une fenêtre de traitement par lots, la fenêtre suivante commence dès que l'invocation de fonction précédente est terminée.

- Pour les sources d'événements Amazon MSK, Apache Kafka autogérées, Amazon MQ et Amazon DocumentDB : la fenêtre de traitement par lots par défaut est de 500 ms. Vous pouvez configurer `MaximumBatchingWindowInSeconds` à n'importe quelle valeur comprise entre 0 et 300 secondes par incréments de secondes. En mode provisionné pour les mappages des sources d'événements Kafka, lorsque vous configurez une fenêtre de traitement par lots, la fenêtre suivante commence dès que le lot précédent est terminé. Dans les mappages des sources d'événements Kafka non provisionnés, si vous configurez une fenêtre de traitement par lots, la fenêtre suivante commence dès que l'invocation de fonction précédente est terminée.

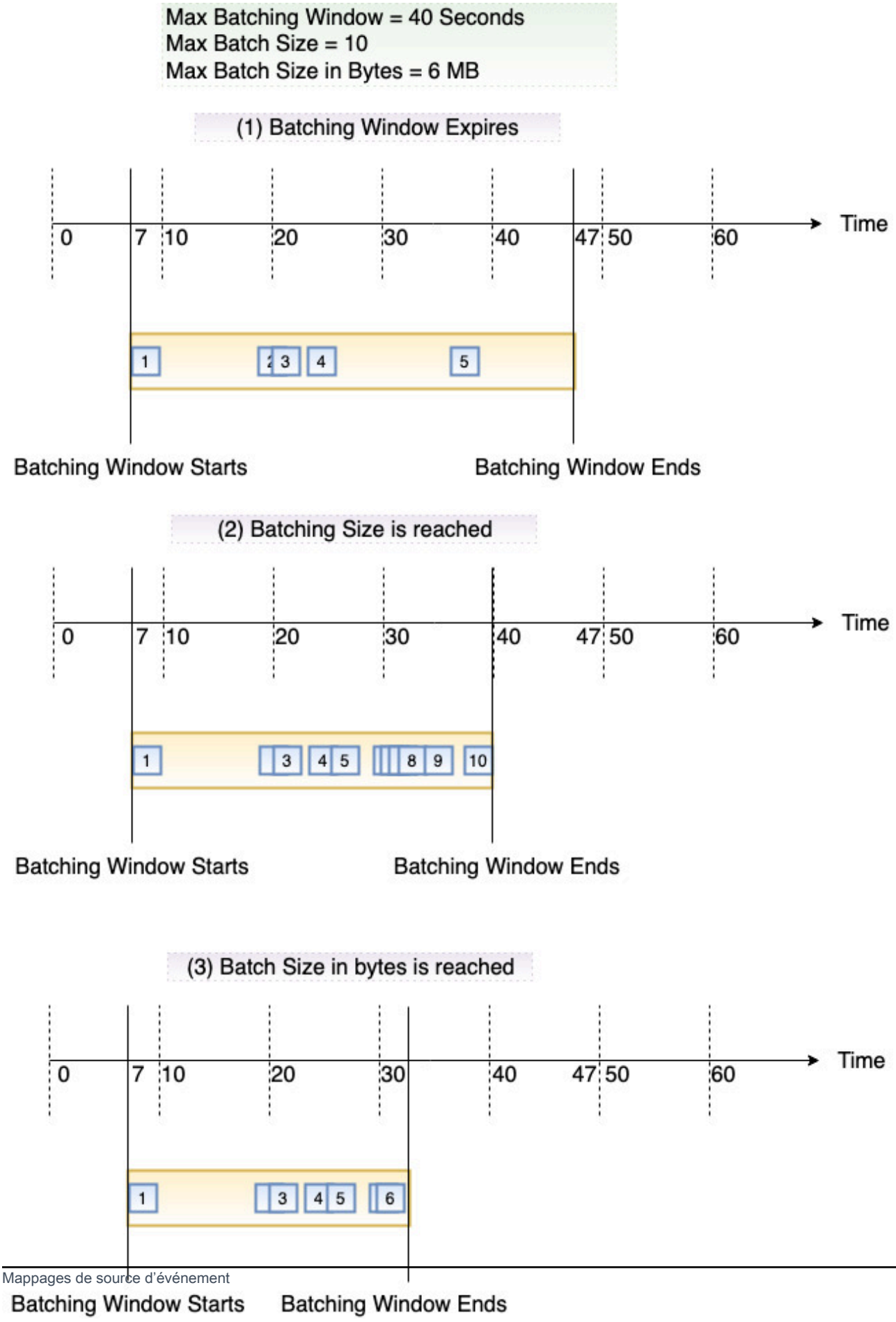
  Pour minimiser la latence lors de l'utilisation des mappages des sources d'événements Kafka en mode provisionné, définissez `MaximumBatchingWindowInSeconds` sur 0. Ce paramètre garantit que Lambda commence à traiter le lot suivant immédiatement après avoir terminé l'appel de fonction en cours. Pour plus d'informations sur le traitement à faible latence, consultez Apache Kafka à faible latence.

- Pour les sources d'événements Amazon MQ et Amazon DocumentDB : la fenêtre de traitement par lots par défaut est de 500 ms. Vous pouvez configurer `MaximumBatchingWindowInSeconds` à n'importe quelle valeur comprise entre 0 et 300 secondes par incréments de secondes. Une fenêtre de traitement par lots commence dès l'arrivée du premier registre.

  > **Note**
  >
  > Étant donné que vous ne pouvez modifier `MaximumBatchingWindowInSeconds` que par incréments de secondes, vous ne pouvez pas revenir à la fenêtre de traitement par lots par défaut de 500 ms après l'avoir modifiée. Pour restaurer la fenêtre de traitement par lots par défaut, vous devez créer un mappage de source d'événement.

- La taille du lot est atteinte. La taille minimale du lot est de 1. La taille par défaut et la taille maximale du lot dépendent de la source d'événement. Pour plus d'informations sur ces valeurs, consultez la spécification BatchSize pour l'opération de l'API `CreateEventSourceMapping`.
- La taille de la charge utile atteint 6 Mo. Vous ne pouvez pas modifier cette limite.

Le diagramme suivant illustre ces trois conditions. Supposons qu'une fenêtre de traitement par lots commence à `t = 7` secondes. Dans le premier scénario, la fenêtre de traitement par lots atteint son maximum de 40 secondes à `t = 47` secondes après avoir accumulé 5 enregistrements. Dans le second scénario, la taille du lot atteint 10 avant l'expiration de la fenêtre de traitement par lots, de sorte que la fenêtre de traitement par lots se termine plus tôt. Dans le troisième scénario, la taille maximale de la charge utile est atteinte avant l'expiration de la fenêtre de traitement par lots, de sorte que la fenêtre de traitement par lots se termine plus tôt.


Max Batching Window = 40 Seconds
Max Batch Size = 10
Max Batch Size in Bytes = 6 MB
(1) Batching Window Expires
0
7
10
20
30
40
47
50
60
Time
1
3
4
5
Batching Window Starts
Batching Window Ends
(2) Batching Size is reached
0
7
10
20
30
40
47
50
60
Time
1
3
4
5
8
9
10
Batching Window Starts
Batching Window Ends
(3) Batch Size in bytes is reached
0
7
10
20
30
40
47
50
60
Time
1
3
4
5
6
Batching Window Starts
Batching Window Ends

Nous vous recommandons de tester avec différentes tailles de lot et d'enregistrement afin que la fréquence d'interrogation de chaque source d'événements soit adaptée à la rapidité avec laquelle votre fonction événementielle est en mesure de terminer sa tâche. Le CreateEventSourceMapping`BatchSize`paramètre contrôle le nombre maximum d'enregistrements qui peuvent être envoyés à votre fonction à chaque appel. Une taille de lot plus grande peut souvent absorber plus efficacement l'invocation sur un plus large ensemble d'enregistrements, ce qui accroît votre débit.

Lambda envoi le prochain lot pour traitement sans attendre que les extensions configurées soient terminées. En d'autres termes, vos extensions peuvent continuer à s'exécuter pendant que Lambda traite le prochain lot d'enregistrements. Cela peut causer des problèmes de limitation si vous enfreignez l'un des paramètres ou l'une des limites de simultanéité de votre compte. Pour détecter s'il s'agit d'un problème éventuel, surveillez vos fonctions et vérifiez si vous observez des métriques de simultanéité plus élevées que prévu pour votre mappage des sources d'événements. En raison de la brièveté des intervalles entre les invocations, Lambda peut brièvement signaler une utilisation simultanée supérieure au nombre de partitions. Cela peut être vrai même pour les fonctions d'événement Lambda sans extensions.

Par défaut, si votre fonction renvoie une erreur, le mappage de la source d'événements retraite l'ensemble du lot jusqu'à ce que la fonction réussisse ou que les éléments du lot arrivent à expiration. Pour s'assurer d'un traitement dans l'ordre, le mappage de la source d'événement met en pause le traitement dans la partition concernée jusqu'à la résolution de l'erreur. Pour les sources de flux (DynamoDB et Kinesis), vous pouvez configurer le nombre maximal de tentatives que Lambda effectue lorsque votre fonction renvoie une erreur. Les erreurs de service ou les limitations où le lot n'atteint pas votre fonction ne comptent pas dans les tentatives de réessai. Vous pouvez également configurer le mappage des sources d'événements pour qu'il envoie un enregistrement d'invocation à une destination lorsqu'il rejette un lot d'événements.

Mode alloué

Les mappages des sources d'événements Lambda utilisent des sondeurs d'événements pour interroger votre source d'événements à la recherche de nouveaux messages. Par défaut, Lambda gère le dimensionnement automatique de ces sondeurs en fonction du volume des messages. Lorsque le trafic de messages augmente, Lambda augmente automatiquement le nombre de sondeurs d'événements pour gérer la charge, et le réduit lorsque le trafic diminue.

En mode provisionné, vous pouvez affiner le débit du mappage de vos sources d'événements en définissant des limites minimales et maximales pour les ressources de sondage dédiées qui restent

prêtes à gérer les modèles de trafic attendus. Ces ressources évoluent automatiquement 3 fois plus vite pour faire face aux pics soudains de trafic d'événements et fournissent une capacité 16 fois supérieure pour traiter des millions d'événements. Cela vous permet de créer des charges de travail hautement réactives axées sur les événements avec des exigences de performance strictes.

Dans Lambda, un sondeur d'événements est une unité de calcul dont les capacités de débit varient selon le type de source d'événements. Pour Amazon MSK et Apache Kafka autogéré, chaque sondeur d'événements peut gérer jusqu'à 5 % MB/sec du débit ou jusqu'à 5 appels simultanés. Par exemple, si votre source d'événement produit une charge utile moyenne de 1 Mo et que la durée moyenne de votre fonction est de 1 seconde, un seul sondeur d'événements Kafka peut prendre en charge 5 MB/sec débits et 5 appels Lambda simultanés (en supposant qu'il n'y ait aucune transformation de charge utile). Pour Amazon SQS, chaque sondeur d'événements peut gérer jusqu'à 1 % MB/sec du débit ou jusqu'à 10 appels simultanés. L'utilisation du mode provisionné entraîne des coûts supplémentaires en fonction de l'utilisation de votre sondeur d'événements. Pour plus d’informations sur la tarification, consultez Tarification AWS Lambda.

Le mode provisionné est disponible pour les sources d'événements Amazon MSK, Apache Kafka autogérées et Amazon SQS. Alors que les paramètres de simultanéité vous permettent de contrôler la mise à l’échelle de votre fonction, le mode alloué vous permet de contrôler le débit de votre mappage des sources d’événements. Pour garantir des performances optimales, vous devrez peut-être ajuster les deux paramètres indépendamment.

Le mode provisionné est idéal pour les applications en temps réel nécessitant une latence constante pour le traitement des événements, telles que les sociétés de services financiers traitant les flux de données du marché, les plateformes de commerce électronique fournissant des recommandations personnalisées en temps réel et les sociétés de jeux gérant les interactions avec les joueurs en direct.

Chaque sondeur d'événements prend en charge une capacité de débit différente :

- Pour Amazon MSK et Apache Kafka autogéré : jusqu'à 5 % MB/sec du débit ou jusqu'à 5 appels simultanés
- Pour Amazon SQS : jusqu'à 1 % MB/sec de débit ou jusqu'à 10 appels simultanés ou jusqu'à 10 appels d'API d'interrogation SQS par seconde.

Pour les mappages de sources d'événements Amazon SQS, vous pouvez définir le nombre minimum de sondeurs entre 2 et 200 avec une valeur par défaut de 2, et le nombre maximum entre 2 et 10 000 avec une valeur par défaut de 200. Lambda adapte le nombre de sondeurs d'événements entre

le minimum et le maximum configurés, en ajoutant rapidement jusqu'à 1 000 appels simultanés par minute afin de fournir un traitement cohérent et à faible latence de vos événements.

Pour les mappages de sources d'événements Kafka, vous pouvez définir le nombre minimum de sondeurs entre 1 et 200 avec une valeur par défaut de 1, et le nombre maximum entre 1 et 2 000 avec une valeur par défaut de 200. Lambda adapte le nombre de sondeurs d'événements entre le minimum et le maximum configurés en fonction de votre historique d'événements dans votre rubrique afin de garantir un traitement à faible latence de vos événements.

Notez que pour les sources d'événements Amazon SQS, le paramètre de simultanéité maximale ne peut pas être utilisé en mode provisionné. Lorsque vous utilisez le mode provisionné, vous contrôlez la simultanéité par le biais du paramètre Nombre maximal de sondeurs d'événements.

Pour plus d’informations sur la configuration du mode alloué, reportez-vous aux sections suivantes :

- Configuration du mode alloué pour les mappages des sources d’événements Amazon MSK
- Configuration du mode alloué pour les mappages des source d’événement Apache Kafka autogéré
- Utilisation du mode provisionné avec les mappages de sources d'événements Amazon SQS

Pour minimiser le temps de latence en mode provisionné, définissez ce paramètre `MaximumBatchingWindowInSeconds` sur 0. Ce paramètre garantit que Lambda commence à traiter le lot suivant immédiatement après avoir terminé l'appel de fonction en cours. Pour plus d’informations sur le traitement à faible latence, consultez Apache Kafka à faible latence.

Après avoir configuré le mode alloué, vous pouvez observer l’utilisation des sondeurs d’événements pour votre charge de travail en surveillant la métrique `ProvisionedPollers`. Pour plus d’informations, consultez the section called “Métriques de mappage des sources d’événements”.

API de mappage de la source d’événement

Pour gérer une source d’événement à l’aide de la AWS Command Line Interface (AWS CLI) ou d’un AWS SDK, vous pouvez utiliser les opérations d’API suivantes :

- CreateEventSourceMapping
- ListEventSourceMappings
- GetEventSourceMapping
- UpdateEventSourceMapping
- DeleteEventSourceMapping

Utilisation des balises dans les mappages des sources d’événements

Vous pouvez étiqueter les mappages des sources d’événements pour organiser et gérer vos ressources. Les balises sont des paires clé-valeur de forme libre associées à vos ressources prises en charge par l’ensemble des ressources Services AWS. Pour plus d'informations sur les cas d'utilisation des balises, consultez la section Stratégies de balisage courantes dans le guide des AWS ressources de balisage et de l'éditeur de balises.

Les mappages de sources d'événements sont associés aux fonctions d'événement, qui peuvent avoir leurs propres balises. Les mappages des sources d’événements n’héritent pas automatiquement des balises des fonctions. Vous pouvez utiliser l' AWS Lambda API pour afficher et mettre à jour les balises. Vous pouvez également consulter et mettre à jour les balises tout en gérant un mappage de source d'événement spécifique dans la console Lambda, y compris ceux utilisant le mode provisionné pour Amazon SQS.

Autorisations requises pour l’utilisation des balises

Pour autoriser une identité Gestion des identités et des accès AWS (IAM) – utilisateur, groupe ou rôle – à afficher ou marquer les ressources, accordez-lui les autorisations correspondantes :

- lambda : ListTags —Lorsqu' une ressource possède des balises, accordez cette autorisation à tous ceux qui ont besoin de `ListTags` l'utiliser. Pour les fonctions d'événement balisées, cette autorisation est également nécessaire pour`GetFunction`.
- lambda : TagResource —Accordez cette autorisation à toute personne ayant besoin d'appeler `TagResource` ou d'exécuter un tag lors de la création.

Vous pouvez éventuellement envisager d'accorder également l'UntagResourceautorisation lambda : pour autoriser les `UntagResource` appels à la ressource.

Pour plus d’informations, consultez Identity-based Politiques IAM pour Lambda.

Utilisation des balises avec la console Lambda

Vous pouvez utiliser la console Lambda pour créer des mappages de sources d'événements comportant des balises, ajouter des balises aux mappages de sources d'événements existants et filtrer les mappages de sources d'événements par balise, y compris ceux configurés en mode provisionné pour Amazon SQS.

Lorsque vous ajoutez un déclencheur pour les services basés sur les flux et les files d’attente pris en charge à l’aide de la console Lambda, Lambda crée automatiquement un mappage des sources

d'événements. Pour plus d'informations sur ces sources d'événements, consultez the section called "Mappages de source d'événement". Pour créer un mappage des sources d'événements dans la console, vous devez remplir les conditions préalables suivantes :

- Une fonction événementielle.
- Une source d'événement provenant d'un service concerné.

Vous pouvez ajouter les balises dans le cadre de l'interface utilisateur que vous utilisez pour créer ou mettre à jour des déclencheurs.

Pour ajouter une balise lors de la création d'un mappage des sources d'événements

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez le nom de votre fonction événementielle.
3. Sous Function overview (Vue d'ensemble de la fonction), choisissez Add trigger (Ajouter un déclencheur).
4. Sous Configuration du déclencheur, dans la liste déroulante, choisissez le nom du service dont provient votre source d'événement.
5. Fournissez la configuration de base de votre source d'événements. Pour plus d'informations sur la configuration de votre source d'événements, consultez la section relative au service correspondant dans the section called "Intégration d'autres services".
6. Sous Configuration du mappage des sources d'événements, sélectionnez Paramètres supplémentaires.
7. Sous Balises, choisissez Ajouter une nouvelle balise.
8. Dans le champ Clé, saisissez la clé de votre balise. Pour plus d'informations sur les restrictions relatives au balisage, consultez la section Limites et exigences relatives au nommage des balises dans le Guide des AWS ressources de balisage et de l'éditeur de balises.
9. Choisissez Ajouter.

Pour ajouter des balises à un mappage des sources d'événements existant

1. Ouvrez la page Mappages des sources d'événements dans la console Lambda.
2. Dans la liste des ressources, choisissez l'UUID du mappage des sources d'événements correspondant à l'ARN de la source d'événement et de la fonction.
3. Dans la liste des onglets située sous le volet de configuration générale, choisissez Balises.

4. Choisissez Gérer les balises.
5. Choisissez Add new tag (Ajouter une nouvelle balise).
6. Dans le champ Clé, saisissez la clé de votre balise. Pour plus d'informations sur les restrictions relatives au balisage, consultez la section Limites et exigences relatives au nommage des balises dans le Guide des AWS ressources de balisage et de l'éditeur de balises.
7. Cliquez sur Enregistrer.

Pour filtrer les mappages des sources d'événements par balise

1. Ouvrez la page Mappages des sources d'événements dans la console Lambda.
2. Cliquez sur la barre de recherche.
3. Dans la liste déroulante, sélectionnez votre clé de balise sous le sous-titre Balises.
4. Sélectionnez Utiliser : « tag-name » pour afficher tous les mappages des sources d'événements étiquetés avec cette touche, ou choisissez un Opérateur pour affiner le filtrage en fonction de la valeur.
5. Sélectionnez votre valeur de balise pour appliquer un filtre combinant la clé et la valeur de la balise.

La zone de recherche prend également en charge la recherche de clés de balise. Saisissez le nom d'une clé pour la rechercher dans la liste.

Utilisation de balises avec AWS CLI

Vous pouvez ajouter et supprimer des balises sur les ressources Lambda existantes, mappages de sources d'événements inclus, avec l'API Lambda. Vous pouvez également ajouter des balises lors de la création d'un mappage de sources d'événements afin de maintenir une ressource étiquetée tout au long de son cycle de vie.

Mise à jour des balises avec les API de balises Lambda

Vous pouvez ajouter et supprimer des balises pour les ressources Lambda prises en charge par le biais des opérations TagResourceet de l'UntagResourceAPI.

Vous pouvez appeler ces opérations par l'intermédiaire de l' AWS CLI. Pour ajouter des balises à une ressource existante, utilisez la commande `tag-resource`. Cet exemple ajoute deux balises, l'une avec la clé *`Department`* et l'autre avec la clé*`CostCenter`*.

```
aws lambda tag-resource \
--resource arn:aws:lambda:us-east-2:123456789012:resource-type:my-resource \
--tags Department=Marketing,CostCenter=1234ABCD
```

Pour supprimer des balises, utilisez la commande `untag-resource`. Cet exemple supprime la balise contenant la clé*`Department`*.

```
aws lambda untag-resource --resource arn:aws:lambda:us-east-1:123456789012:resource-type:resource-identifier \
--tag-keys Department
```

Ajout de balises lors de la création d'un mappage des sources d'événements

Pour créer un nouveau mappage de source d'événements Lambda avec des balises, utilisez l'opération CreateEventSourceMappingAPI. Spécifiez le paramètre `Tags`. Vous pouvez appeler cette opération à l'aide de la `create-event-source-mapping` AWS CLI commande et de l'`--tags`option. Pour plus d'informations sur la commande de la CLI, consultez create-event-source-mapping dans la Référence des commandes de l'AWS CLI .

Avant d'utiliser le paramètre `Tags` avec `CreateEventSourceMapping`, vérifiez que votre rôle dispose de l'autorisation d'étiqueter les ressources en plus des autorisations habituelles nécessaires à cette opération. Pour plus d'informations sur les autorisations requises pour l'étiquetage, consultez the section called "Autorisations requises pour l'utilisation des balises".

Affichage des balises avec les API de balises Lambda

Pour afficher les balises associées à une ressource Lambda spécifique, utilisez l'opération d'API `ListTags`. Pour plus d'informations, consultez ListTags.

Vous pouvez appeler cette opération à l'aide de la `list-tags` AWS CLI commande en fournissant un ARN (Amazon Resource Name).

```
aws lambda list-tags --resource arn:aws:lambda:us-east-1:123456789012:resource-type:resource-identifier
```

Filtrage de ressources par balise

Vous pouvez utiliser le fonctionnement de l' AWS Resource Groups Tagging API GetResourcesAPI pour filtrer vos ressources par balises. L'opération `GetResources` reçoit jusqu'à 10 filtres,

chaque filtre contenant une clé de balise et jusqu'à 10 valeurs de balise. Vous fournissez `GetResources`avec un `ResourceType` pour filtrer par certains types de ressources.

Vous pouvez appeler cette opération à l'aide de la `get-resources` AWS CLI commande. Pour des exemples d'utilisation de `get-resources`, consultez get-resources dans la Référence des commandes de l'AWS CLI.

Contrôlez les événements que Lambda envoie à votre fonction d'événement

Vous pouvez utiliser le filtrage d'événements pour contrôler les enregistrements d'un flux ou d'une file d'attente que Lambda envoie à votre fonction. Par exemple, vous pouvez ajouter un filtre pour que votre fonction ne traite que les messages Amazon SQS contenant certains paramètres de données. Le filtrage des sources d'événements ne fonctionne qu'avec certains mappages des sources d'événements. Vous pouvez ajouter des filtres aux mappages de sources d'événements pour les éléments suivants : Services AWS

- Amazon DynamoDB
- Amazon Kinesis Data Streams
- Amazon MQ
- Amazon Managed Streaming for Apache Kafka (Amazon MSK)
- Self-managed Apache Kafka
- Amazon Simple Queue Service (Amazon SQS)

Pour obtenir des informations spécifiques sur le filtrage avec des sources d'événements précises, consultez the section called "Utilisation de filtres avec différents Services AWS". Lambda ne prend pas en charge le filtrage d'événements pour Amazon DocumentDB.

Par défaut, vous pouvez définir jusqu'à cinq filtres différents pour un seul mappage des sources d'événements. Vos filtres sont logiquement combinés par OU. Si un enregistrement de votre source d'événement satisfait un ou plusieurs de vos filtres, Lambda inclut l'enregistrement dans le prochain événement qu'il envoie à votre fonction. Si aucun de vos filtres n'est satisfait, Lambda rejette l'enregistrement.

> **Note**
>
> Si vous avez besoin de définir plus de cinq filtres pour une source d'événement, vous pouvez demander une augmentation de quota jusqu'à dix filtres pour chaque source d'événement. Si vous essayez d'ajouter plus de filtres que ne le permet votre quota actuel, Lambda renvoie une erreur lorsque vous essayez de créer la source d'événement.

Rubriques

- Présentation des principes de base du filtrage d'événements

- Traitement des enregistrements ne répondant pas aux critères de filtrage
- Syntaxe des règles de filtrage
- Attacher des critères de filtre à un mappage de sources d'événements (console)
- Associer des critères de filtre à un mappage de source d'événement (AWS CLI)
- Associer des critères de filtre à un mappage de source d'événement (AWS SAM)
- Chiffrement des critères de filtre
- Utilisation de filtres avec différents Services AWS

Présentation des principes de base du filtrage d'événements

Un objet (`FilterCriteria`) de critères de filtre est une structure composée d'une liste de filtres (`Filters`). Chaque filtre est une structure qui définit un modèle de filtrage d'événements (`Pattern`). Un modèle est une représentation sous forme de chaîne d'une règle de filtre JSON. La structure d'un objet `FilterCriteria` est la suivante.

```
{
   "Filters": [
        {
            "Pattern": "{ \"Metadata1\": [ rule1 ], \"data\": { \"Data1\":
 [ rule2 ] }}"
        }
    ]
}
```

Pour plus de clarté, voici la valeur du `Pattern` de filtre étendu en JSON simple :

```
{
    "Metadata1": [ rule1 ],
    "data": {
        "Data1": [ rule2 ]
    }
}
```

Votre modèle de filtrage peut inclure des propriétés de métadonnées, des propriétés de données ou les deux. Les paramètres de métadonnées disponibles et le format des paramètres de données varient en fonction de l'objet Service AWS qui sert de source d'événements. Par exemple, supposons que votre mappage des sources d'événements reçoit l'enregistrement suivant d'une file d'attente Amazon SQS :

```
{
    "messageId": "059f36b4-87a3-44ab-83d2-661975830a7d",
    "receiptHandle": "AQEBwJnKyrHigUMZj6rYigCgxlaS3SLy0a...",
    "body": "{\\n \"City\": \"Seattle\",\\n \"State\": \"WA\",\\n \"Temperature\":
 \"46\"\\n}",
    "attributes": {
        "ApproximateReceiveCount": "1",
        "SentTimestamp": "1545082649183",
        "SenderId": "AIDAIENQZJOLO23YVJ4VO",
        "ApproximateFirstReceiveTimestamp": "1545082649185"
    },
    "messageAttributes": {},
    "md5OfBody": "e4e68fb7bd0e697a0ae8f1bb342846b3",
    "eventSource": "aws:sqs",
    "eventSourceARN": "arn:aws:sqs:us-east-2:123456789012:my-queue",
    "awsRegion": "us-east-2"
}
```

- Les propriétés de métadonnées sont les champs contenant des informations sur l'événement qui a créé l'enregistrement. Dans l'exemple d'enregistrement Amazon SQS, les propriétés de métadonnées comprennent des champs tels que `messageID`, `eventSourceArn` et `awsRegion`.
- Les propriétés de données sont les champs de l'enregistrement contenant les données de votre flux ou file d'attente. Dans l'exemple d'événement Amazon SQS, la clé du champ de données est `body` et les propriétés de données sont les champs `City` `State` et `Temperature`.

Les différents types de sources d'événements utilisent des valeurs clés différentes pour leurs champs de données. Pour filtrer en fonction des propriétés des données, assurez-vous d'utiliser la bonne clé dans le modèle de votre filtre. Pour obtenir la liste des clés de filtrage des données et des exemples de modèles de filtre pris en charge pour chacune d'entre elles Service AWS, reportez-vous àUtilisation de filtres avec différents Services AWS.

Le filtrage d'événements peut gérer le filtrage JSON à plusieurs niveaux. Par exemple, considérez le fragment suivant d'un enregistrement provenant d'un flux DynamoDB :

```
"dynamodb": {
    "Keys": {
        "ID": {
            "S": "ABCD"
        }
        "Number": {
```

```
            "N": "1234"
    },
    ...
}
```

Supposons que vous vouliez traiter uniquement les enregistrements dont la valeur de la clé de tri `Number` est 4 567. Dans ce cas, votre objet `FilterCriteria` se présente comme suit :

```
{
    "Filters": [
        {
            "Pattern": "{ \"dynamodb\": { \"Keys\": { \"Number\": { \"N\":
 [ "4567" ] } } } }"
        }
    ]
}
```

Pour plus de clarté, voici la valeur du `Pattern` de filtre étendu en JSON simple :

```
{
    "dynamodb": {
        "Keys": {
            "Number": {
                "N": [ "4567" ]
                }
            }
        }
}
```

Traitement des enregistrements ne répondant pas aux critères de filtrage

La manière dont Lambda gère les enregistrements qui ne répondent pas à vos critères de filtre dépend de la source de l'événement.

- Pour Amazon SQS, si un message ne répond pas à vos critères de filtre, Lambda supprime automatiquement le message de la file d'attente. Vous n'avez pas besoin de supprimer manuellement ces messages dans Amazon SQS.
- Pour Kineses et DynamoDB, après que vos critères de filtre ont évalué un enregistrement, l'itérateur de flux avance au-delà de cet enregistrement. Si l'enregistrement ne répond pas à vos critères de filtre, vous n'avez pas besoin de supprimer manuellement l'enregistrement de la source de votre événement. Après la période de conservation, Kinesis et DynamoDB suppriment

automatiquement ces anciens enregistrements. Si vous souhaitez que les enregistrements soient supprimés plus tôt, consultez Modification de la période de conservation des données.

- Pour les messages Amazon MSK, Apache Kafka autogéré et Amazon MQ, Lambda supprime les messages qui ne correspondent pas à tous les champs inclus dans le filtre. Pour Amazon MSK et Apache Kafka autogéré, Lambda valide les décalages pour les messages correspondants et non correspondants après avoir invoqué avec succès la fonction d'événement. Pour Amazon MQ, Lambda accuse réception des messages correspondants après avoir correctement invoqué la fonction et reconnaît les messages non correspondants lors du filtrage.

Syntaxe des règles de filtrage

Pour les règles de filtrage, Lambda prend en charge EventBridge les règles Amazon et utilise la même syntaxe que. EventBridge Pour plus d'informations, consultez les modèles EventBridge d'événements Amazon dans le guide de EventBridge l'utilisateur Amazon.

Voici un récapitulatif de tous les opérateurs de comparaison disponibles pour le filtrage d’événement Lambda.

Opérateur de comparaison	Exemple	Syntaxe des règles
Null	UserID est null	"UserID": [null]
Vide	LastName est vide	"LastName": [""]
Égal à	Le nom est « Alice »	"Name": ["Alice"]
Est égal à (ignorer les majuscules)	Le nom est « Alice »	"Name": [{ "equals-ignore-case": "alice" }]
Et	Le lieu est « New York » et le jour est « Monday »	"Location": ["New York"], "Day": ["Monday"]
Or	PaymentType est « Crédit » ou « Débit »	PaymentType« : [« Crédit », « Débit"]
Ou (plusieurs champs)	Location est « New York », ou Day est « Monday ».	"$or": [{ "Location": ["New York"] }, { "Day": ["Monday"] }]

Opérateur de comparaison	Exemple	Syntaxe des règles
Pas	La météo est tout sauf « Raining »	"Weather": [{ "anything-but": ["Raining"] }]
Numérique (égal)	Le prix est de 100	"Price": [{ "numeric": ["=", 100] }]
Numérique (plage)	Le prix est supérieur à 10 et inférieur ou égal à 20	"Price": [{ "numeric": [">", 10, "<=", 20] }]
Existe	ProductName existe	ProductName« : [{« existe » : vrai}]
N'existe pas	ProductName n'existe pas	ProductName« : [{« existe » : faux}]
Commence par	La région se trouve aux États-Unis	"Region": [{"prefix": "us-" }]
Termine par	FileName se termine par une extension .png.	FileName« : [{« suffixe » : « .png »}]

> **Note**
>
> Comme pour les chaînes EventBridge, Lambda utilise une correspondance exacte caractère par caractère sans mise en majuscules ni aucune autre normalisation de chaîne. Pour les nombres, Lambda utilise également une représentation par chaîne. Par exemple, 300, 300,0 et 3.0e2 ne sont pas considérés égaux.

Notez que l'opérateur Exists ne fonctionne que sur les nœuds feuilles de votre source d'événements JSON. Il ne tient pas compte des nœuds intermédiaires. Par exemple, avec le JSON suivant, le modèle de filtre `{ "person": { "address": [ { "exists": true } ] } }` ne trouverait aucune correspondance, car `"address"` est un nœud intermédiaire.

```
{
  "person": {
```

```
    "name": "John Doe",
    "age": 30,
    "address": {
      "street": "123 Main St",
      "city": "Anytown",
      "country": "USA"
    }
  }
}
```

Attacher des critères de filtre à un mappage de sources d'événements (console)

Suivez ces étapes pour créer un nouveau mappage de source d'événement avec des critères de filtre à l'aide de la console Lambda.

Pour créer un nouveau mappage de sources d'événements avec des critères de filtre (console)

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez le nom d'une fonction d'événement pour laquelle créer un mappage de source d'événement.
3. Sous Function overview (Vue d'ensemble de la fonction), choisissez Add trigger (Ajouter un déclencheur).
4. Pour Trigger configuration (Configuration du déclencheur), choisissez un type de déclencheur qui prend en charge le filtrage des événements. Pour obtenir la liste des services pris en charge, reportez-vous à la liste figurant au début de cette page.
5. Développer Additional settings (Paramètres supplémentaires).
6. Sous Filter criteria (Critères de filtre), choisissez Add (Ajouter) puis définissez et saisissez vos filtres. Par exemple, vous pouvez saisir ce qui suit.

   ```
   { "Metadata" : [ 1, 2 ] }
   ```

   Cela indique à Lambda de traiter uniquement les enregistrements où le champ `Metadata` est égal à 1 ou 2. Vous pouvez continuer à sélectionner Ajouter pour ajouter d'autres filtres jusqu'à la quantité maximale autorisée.
7. Lorsque vous avez terminé d'ajouter vos filtres, sélectionnez Enregistrer.

Lorsque vous saisissez des critères de filtrage à l'aide de la console, vous n'entrez que le modèle de filtrage et n'avez pas besoin d'indiquer la touche `Pattern` ni d'échapper aux guillemets. À l'étape 6 des instructions précédentes, `{ "Metadata" : [ 1, 2 ] }` correspond à ce qui suit `FilterCriteria`.

```
{
   "Filters": [
      {
          "Pattern": "{ \"Metadata\" : [ 1, 2 ] }"
      }
   ]
}
```

Après avoir créé le mappage de la source d'événements dans la console, vous pouvez voir les `FilterCriteria` formatés dans les détails du déclencheur. Pour plus d'exemples de création de filtres d'événements à l'aide de la console, consultez Utilisation de filtres avec différents Services AWS.

Associer des critères de filtre à un mappage de source d'événement (AWS CLI)

Supposons que vous souhaitiez que le mappage d'une source d'événements comporte les suivants `FilterCriteria`:

```
{
   "Filters": [
      {
          "Pattern": "{ \"Metadata\" : [ 1, 2 ] }"
      }
   ]
}
```

Pour créer un nouveau mappage de source d'événements avec ces critères de filtre à l'aide de AWS Command Line Interface (AWS CLI), exécutez la commande suivante.

```
aws lambda create-event-source-mapping \
    --function-name my-function \
    --event-source-arn arn:aws:sqs:us-east-2:123456789012:my-queue \
    --filter-criteria '{"Filters": [{"Pattern": "{ \"Metadata\" : [ 1, 2 ]}"}]}'
```

Cette commande create-event-source-mapping crée un mappage des sources d'événements Amazon SQS pour la fonction `my-function` avec les `FilterCriteria` spécifiés.

Pour ajouter ces critères de filtre à un mappage des sources d'événements existant, exécutez la commande suivante.

```
aws lambda update-event-source-mapping \
    --uuid "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE" \
    --filter-criteria '{"Filters": [{"Pattern": "{ \"Metadata\" : [ 1, 2 ]}"}]}'
```

Notez que pour mettre à jour un mappage de source d'événements, vous avez besoin de son UUID. Vous pouvez obtenir l'UUID à l'aide d'un appel list-event-source-mappings. Lambda renvoie également l'UUID dans la réponse create-event-source-mapping de la CLI.

Pour supprimer les critères de filtre d'une source d'événements, vous pouvez exécuter la commande update-event-source-mapping suivante avec un objet `FilterCriteria` vide.

```
aws lambda update-event-source-mapping \
    --uuid "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE" \
    --filter-criteria "{}"
```

Pour plus d'exemples de création de filtres d'événements à l'aide du AWS CLI, voirUtilisation de filtres avec différents Services AWS.

Associer des critères de filtre à un mappage de source d'événement (AWS SAM)

Supposons que vous souhaitiez configurer une source d'événements AWS SAM pour utiliser les critères de filtre suivants :

```
{
   "Filters": [
      {
          "Pattern": "{ \"Metadata\" : [ 1, 2 ] }"
      }
   ]
}
```

Pour ajouter ces critères de filtre à votre mappage des sources d'événements, insérez l'extrait suivant dans le modèle YAML de votre source d'événements.

```
FilterCriteria:
  Filters:
    - Pattern: '{"Metadata": [1, 2]}'
```

Pour plus d'informations sur la création et la configuration d'un AWS SAM modèle pour un mappage de sources d'événements, consultez la EventSourcesection du guide du AWS SAM développeur. Pour plus d'exemples de création de filtres d'événements à l'aide AWS SAM de modèles, consultezUtilisation de filtres avec différents Services AWS.

Chiffrement des critères de filtre

Par défaut, Lambda ne chiffre pas votre objet de critères de filtre. Dans les cas d'utilisation où vous pourriez inclure des informations sensibles dans votre objet de critères de filtre, vous pouvez utiliser votre propre clé KMS pour les chiffrer.

Une fois que vous avez chiffré votre objet de critères de filtre, vous pouvez afficher sa version en texte brut à l'aide d'un appel d'GetEventSourceMappingAPI. Vous devez disposer des autorisations `kms:Decrypt` nécessaires pour afficher correctement les critères de filtre en texte brut.

> **Note**
>
> Si votre objet de critères de filtre est chiffré, Lambda expédie la valeur du `FilterCriteria` champ dans la réponse aux appels. ListEventSourceMappings Ce champ s'affiche plutôt sous la forme `null`. Pour connaître la vraie valeur de`FilterCriteria`, utilisez l'GetEventSourceMappingAPI.
> Pour afficher la valeur déchiffrée de `FilterCriteria` dans la console, assurez-vous que votre rôle IAM contient des autorisations pour. GetEventSourceMapping

Vous pouvez spécifier votre propre clé KMS via la console API/CLI, ou CloudFormation.

Pour chiffrer les critères de filtre à l'aide d'une clé KMS appartenant au client (console)

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez Add trigger (Ajouter déclencheur). Si vous possédez déjà un déclencheur, choisissez l'onglet Configuration, puis sur Déclencheurs. Sélectionnez le déclencheur existant, puis choisissez Modifier.
3. Cochez la case en regard de Chiffrer avec une clé KMS gérée par le client.
4. Pour Choisir une clé de chiffrement KMS gérée par le client, sélectionnez une clé activée existante ou créez-en une. Selon l'opération, vous avez besoin de certaines ou de toutes les autorisations suivantes : `kms:DescribeKey`, `kms:GenerateDataKey` et `kms:Decrypt`. Utilisez la stratégie de clé KMS pour octroyer ces autorisations.

Si vous utilisez votre propre clé KMS, les opérations d'API suivantes doivent être autorisées dans la stratégie de clé :

- `kms:Decrypt` : doit être octroyé au principal du service Lambda régional (`lambda.AWS_region.amazonaws.com`). Cela permet à Lambda de déchiffrer les données avec cette clé KMS.
  - Pour éviter un problème des adjoints confus entre services, la stratégie de clé utilise la clé de condition globale `aws:SourceArn`. La valeur correcte de la clé `aws:SourceArn` est l'ARN de votre ressource de mappage des sources d'événements. Vous ne pouvez donc l'ajouter à votre stratégie qu'une fois que vous connaissez son ARN. Lambda transmet également les clés `aws:lambda:FunctionArn` et `aws:lambda:EventSourceArn`, ainsi que leurs valeurs respectives dans le contexte de chiffrement lors d'une requête de déchiffrement à KMS. Ces valeurs doivent correspondre aux conditions spécifiées dans la stratégie de clé pour que la requête de déchiffrement aboutisse. Vous n'avez pas besoin d'inclure EventSourceArn les sources d'événements de Self-managed Kafka puisqu'elles n'ont pas de EventSourceArn.
- `kms:Decrypt`— Doit également être accordé au principal qui a l'intention d'utiliser la clé pour afficher les critères de filtrage en texte brut dans les appels GetEventSourceMappingd'DeleteEventSourceMappingAPI.
- `kms:DescribeKey` : fournit les détails des clés gérées par le client pour permettre au principal spécifié d'utiliser la clé.
- `kms:GenerateDataKey` :permet à Lambda de générer une clé de données pour chiffrer les critères de filtre, au nom du principal spécifié (chiffrement d'enveloppe).

Vous pouvez l'utiliser AWS CloudTrail pour suivre les AWS KMS demandes que Lambda effectue en votre nom. Pour des exemples CloudTrail d'événements, voir???.

Nous recommandons également d'utiliser la clé de condition `kms:ViaService` pour limiter l'utilisation de la clé KMS aux requêtes ne provenant que de Lambda. La valeur de cette clé est le principal de service Lambda régional (`lambda.AWS_region.amazonaws.com`). Voici un exemple de stratégie de clé qui accorde toutes les autorisations pertinentes :

Example AWS KMS politique clé

JSON

```
{
    "Version":"2012-10-17",
```

```
    "Id": "example-key-policy-1",
    "Statement": [
        {
            "Sid": "Allow Lambda to decrypt using the key",
            "Effect": "Allow",
            "Principal": {
                "Service": "lambda.us-east-1.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": "*",
            "Condition": {
                "ArnEquals" : {
                    "aws:SourceArn": [
                        "arn:aws:lambda:us-east-1:123456789012:event-source-
mapping:<esm_uuid>"
                    ]
                },
                "StringEquals": {

 "kms:EncryptionContext:aws:lambda:FunctionArn": "arn:aws:lambda:us-
east-1:123456789012:function:test-function",

 "kms:EncryptionContext:aws:lambda:EventSourceArn": "arn:aws:sqs:us-
east-1:123456789012:test-queue"
                }
            }
        },
        {
            "Sid": "Allow actions by an AWS account on the key",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Allow use of the key to specific roles",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:role/ExampleRole"
            },
```

```
            "Action": [
                "kms:Decrypt",
                "kms:DescribeKey",
                "kms:GenerateDataKey"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals" : {
                    "kms:ViaService": "lambda.us-east-1.amazonaws.com"
                }
            }
        }
    ]
}
```

Pour utiliser votre propre clé KMS afin de chiffrer les critères de filtre, vous pouvez également utiliser la CreateEventSourceMapping AWS CLI commande suivante. Spécifiez l'ARN de la clé KMS avec l'option `--kms-key-arn`.

```
aws lambda create-event-source-mapping --function-name my-function \
    --maximum-batching-window-in-seconds 60 \
    --event-source-arn arn:aws:sqs:us-east-1:123456789012:my-queue \
    --filter-criteria "{\"filters\": [{\"pattern\": \"{\"a\": [\"1\", \"2\"]}\" }]}" \
    --kms-key-arn arn:aws:kms:us-east-1:123456789012:key/055efbb4-xmpl-4336-
ba9c-538c7d31f599
```

Si vous disposez déjà d'un mappage de source d'événements, utilisez plutôt la UpdateEventSourceMapping AWS CLI commande. Spécifiez l'ARN de la clé KMS avec l'option `--kms-key-arn`.

```
aws lambda update-event-source-mapping --function-name my-function \
    --maximum-batching-window-in-seconds 60 \
    --event-source-arn arn:aws:sqs:us-east-1:123456789012:my-queue \
    --filter-criteria "{\"filters\": [{\"pattern\": \"{\"a\": [\"1\", \"2\"]}\" }]}" \
    --kms-key-arn arn:aws:kms:us-east-1:123456789012:key/055efbb4-xmpl-4336-
ba9c-538c7d31f599
```

Cette opération remplace toute clé KMS précédemment spécifiée. Si vous spécifiez l'option `--kms-key-arn` avec un argument vide, Lambda cesse d'utiliser votre clé KMS pour chiffrer les critères de filtre. Au lieu de cela, Lambda utilise à nouveau une clé par défaut. Amazon-owned

Pour spécifier votre propre clé KMS dans un CloudFormation modèle, utilisez la `KMSKeyArn` propriété du type de `AWS::Lambda::EventSourceMapping` ressource. Par exemple, vous pouvez insérer l'extrait de code suivant dans le modèle YAML de votre source d'événement.

```
MyEventSourceMapping:
  Type: AWS::Lambda::EventSourceMapping
  Properties:
    ...
    FilterCriteria:
      Filters:
        - Pattern: '{"a": [1, 2]}'
    KMSKeyArn: "arn:aws:kms:us-east-1:123456789012:key/055efbb4-xmpl-4336-
ba9c-538c7d31f599"
    ...
```

Pour pouvoir afficher vos critères de filtre chiffrés en texte clair dans un appel d'DeleteEventSourceMappingAPI GetEventSourceMappingou un appel d'API, vous devez disposer d'`kms:Decrypt`autorisations.

À compter du 6 août 2024, le `FilterCriteria` champ n'apparaît plus dans les AWS CloudTrail journaux provenant de CreateEventSourceMappinget dans UpdateEventSourceMappingles appels d'DeleteEventSourceMappingAPI si votre fonction n'utilise pas le filtrage des événements. Si votre fonction utilise le filtrage des événements, le champ `FilterCriteria` apparaît vide (`{}`). Vous pouvez toujours afficher vos critères de filtre en texte clair en réponse aux appels d'GetEventSourceMappingAPI si vous êtes autorisé à `kms:Decrypt` utiliser la bonne clé KMS.

Exemple d'entrée de CloudTrail journal pour les Create/Update/DeleteEventSourceMapping appels

Dans l' AWS CloudTrail exemple d'entrée de journal suivant pour un CreateEventSourceMapping appel, `FilterCriteria` apparaît comme vide (`{}`) car la fonction utilise le filtrage des événements. C'est le cas même si l'objet `FilterCriteria` contient des critères de filtre valides que votre fonction utilise activement. Si la fonction n'utilise pas le filtrage des événements, le `FilterCriteria` champ CloudTrail n'apparaîtra pas du tout dans les entrées du journal.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROA123456789EXAMPLE:userid1",
        "arn": "arn:aws:sts::123456789012:assumed-role/Example/example-role",
        "accountId": "123456789012",
```

```
        "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROA987654321EXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/User1",
                "accountId": "123456789012",
                "userName": "User1"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2024-05-09T20:35:01Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2024-05-09T21:05:41Z",
    "eventSource": "lambda.amazonaws.com",
    "eventName": "CreateEventSourceMapping20150331",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "eventSourceArn": "arn:aws:sqs:us-east-2:123456789012:example-queue",
        "functionName": "example-function",
        "enabled": true,
        "batchSize": 10,
        "filterCriteria": {},
        "kMSKeyArn": "arn:aws:kms:us-east-2:123456789012:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
        "scalingConfig": {},
        "maximumBatchingWindowInSeconds": 0,
        "sourceAccessConfigurations": []
    },
    "responseElements": {
        "uUID": "a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa",
        "batchSize": 10,
        "maximumBatchingWindowInSeconds": 0,
        "eventSourceArn": "arn:aws:sqs:us-east-2:123456789012:example-queue",
        "filterCriteria": {},
        "kMSKeyArn": "arn:aws:kms:us-east-2:123456789012:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
```

```
        "functionArn": "arn:aws:lambda:us-east-2:123456789012:function:example-
function",
        "lastModified": "May 9, 2024, 9:05:41 PM",
        "state": "Creating",
        "stateTransitionReason": "USER_INITIATED",
        "functionResponseTypes": [],
        "eventSourceMappingArn": "arn:aws:lambda:us-east-2:123456789012:event-source-
mapping:a1b2c3d4-5678-90ab-cdef-EXAMPLEbbbbb"
    },
    "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
    "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "sessionCredentialFromConsole": "true"
}
```

Utilisation de filtres avec différents Services AWS

Les différents types de sources d'événements utilisent des valeurs clés différentes pour leurs champs de données. Pour filtrer en fonction des propriétés des données, assurez-vous d'utiliser la bonne clé dans le modèle de votre filtre. Le tableau suivant indique les clés de filtrage pour chacune des clés prises en charge Service AWS.

Service AWS	Clé de filtrage
DynamoDB	`dynamodb`
Kinesis	`data`
Amazon MQ	`data`
Amazon MSK	`value`
Self-managed Apache Kafka	`value`
Amazon SQS	`body`

Les sections suivantes donnent des exemples de modèles de filtre pour différents types de sources d'événements. Elles fournissent également des définitions des formats de données entrantes pris en charge et des formats de corps de modèle de filtre pour chaque service pris en charge.

- the section called "Filtrage des événements"
- the section called "Filtrage des événements"
- the section called "Filtrage des événements"
- the section called "Filtrage des événements"
- the section called "Filtrage des événements"

Test des fonctions d'événement Lambda dans la console

Vous pouvez tester vos fonctions d'événement Lambda dans la console en appelant votre fonction avec un événement de test. Un événement de test est une entrée JSON dans votre fonction d'événement. Si votre fonction ne nécessite pas d'entrée, l'événement peut être un document vide (`{}`).

Lorsque vous exécutez un test dans la console, Lambda invoque votre fonction de manière synchrone avec l'événement de test. L'exécution de la fonction convertit le JSON de l'événement en un objet et le transmet à la méthode du gestionnaire de votre code afin qu'il soit traité.

> **Créer un événement de test**
>
> Avant de pouvoir tester dans la console, vous devez créer un événement de test privé ou partageable.

Invocation de fonctions d'événement avec des événements de test

Pour tester une fonction événementielle

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez le nom de la fonction d'événement que vous souhaitez tester.
3. Choisissez l'onglet Test.
4. Sous Test event (Événement de test), sélectionnez Create new event (Créer un nouvel événement) ou Edit saved event (Modifier un événement sauvegardé), puis sélectionnez l'événement sauvegardé que vous voulez utiliser.
5. En option, choisissez un modèle pour le JSON de l'événement.
6. Sélectionnez Tester).
7. Pour examiner les résultats du test, sous Execution result (Résultat de l'exécution), développez Details (Détails).

Pour appeler votre fonction d'événement sans enregistrer votre événement de test, choisissez Test avant de l'enregistrer. Cela crée un événement de test non sauvegardé que Lambda ne conserve que pour la durée de la session.

Pour les Node.js environnements d'exécution Python et Ruby, vous pouvez également accéder à vos événements de test enregistrés et non enregistrés dans l'onglet Code. Utilisez la section ÉVÉNEMENTS DE TEST pour créer, modifier et exécuter des tests.

Création d’événements de test privés

Les événements de test privés sont disponibles uniquement pour le créateur de l’événement et ils ne nécessitent aucune autorisation supplémentaire pour être utilisés. Vous pouvez créer et enregistrer jusqu'à 10 événements de test privés par fonction d'événement.

Pour créer un événement de test privé

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez le nom de la fonction d'événement que vous souhaitez tester.
3. Choisissez l’onglet Test.
4. Sous Test event (Événement de test), procédez comme suit :
    a. Choisissez un Template (Modèle).
    b. Saisissez un Name (Nom) pour le test.
    c. Dans la zone de saisie de texte, entrez l’événement de test JSON.
    d. Sous Event sharing settings (Paramètres de partage de l’événement), choisissez Private (Privé).
5. Cliquez sur Enregistrer les modifications.

Pour les Node.js environnements d'exécution Python et Ruby, vous pouvez également créer des événements de test dans l'onglet Code. Utilisez la section ÉVÉNEMENTS DE TEST pour créer, modifier et exécuter des tests.

Création d’événements de test partageables

Les événements de test partageables sont des événements de test que vous pouvez partager avec d'autres utilisateurs du même AWS compte. Vous pouvez modifier les événements de test partageables par d'autres utilisateurs et invoquer votre fonction d'événement avec eux.

Lambda enregistre les événements de test partageables sous forme de schémas dans un registre de schémas Amazon EventBridge (CloudWatch Events) nommé. `lambda-testevent-schemas` Comme Lambda utilise ce registre pour stocker et appeler les événements de test partageables que

vous créez, nous vous recommandons de ne pas modifier ce registre ni d'en créer un en utilisant le nom. `lambda-testevent-schemas`

Pour consulter, partager et modifier des événements de test partageables, vous devez disposer d'autorisations pour toutes les opérations d'API de registre de schéma EventBridge (CloudWatch événements) suivantes :

- schémas. CreateRegistry
- schémas. CreateSchema
- schémas. DeleteSchema
- schémas. DeleteSchemaVersion
- schémas. DescribeRegistry
- schémas. DescribeSchema
- schémas. GetDiscoveredSchema
- schémas. ListSchemaVersions
- schémas. UpdateSchema

Notez que l'enregistrement des modifications apportées à un événement de test partageable remplace cet événement.

Si vous ne pouvez pas créer, modifier ou consulter des événements de test partageables, vérifiez que votre compte dispose des autorisations requises pour ces opérations. Si vous disposez des autorisations requises mais que vous ne pouvez toujours pas accéder aux événements de test partageables, vérifiez s'il existe des politiques basées sur les ressources susceptibles de limiter l'accès au registre EventBridge (des CloudWatch événements).

Pour créer un événement de test partageable

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez le nom de la fonction d'événement que vous souhaitez tester.
3. Choisissez l'onglet Test.
4. Sous Test event (Événement de test), procédez comme suit :
    a. Choisissez un Template (Modèle).
    b. Saisissez un Name (Nom) pour le test.
    c. Dans la zone de saisie de texte, entrez l'événement de test JSON.

d. Sous Event sharing settings (Paramètres de partage de l'événement), choisissez Shareable (Partageable).

5. Cliquez sur Enregistrer les modifications.

> Utilisez des événements de test partageables avec AWS Serverless Application Model.
>
> Vous pouvez l'utiliser AWS SAM pour invoquer des événements de test partageables. Voir Sam Remote Test-Event dans le manuel du développeur AWS Serverless Application Model

Suppression des schémas d'événements de test partageables

Lorsque vous supprimez des événements de test partageables, Lambda les supprime du registre `lambda-testevent-schemas`. Si vous supprimez le dernier événement de test partageable du registre, Lambda supprime le registre.

Si vous supprimez la fonction d'événement, Lambda ne supprime aucun schéma d'événement de test partageable associé. Vous devez nettoyer ces ressources manuellement depuis la console EventBridge (CloudWatch Events).

États de la fonction d'événement Lambda

Lambda inclut un champ d'état dans la configuration de la fonction pour toutes les fonctions d'événement afin d'indiquer quand votre fonction est prête à être invoquée. `State`fournit des informations sur l'état actuel de la fonction, notamment sur la possibilité d'invoquer la fonction avec succès. Les états de la fonction d'événement ne modifient pas le comportement des appels de fonctions ni la façon dont votre fonction exécute le code.

> **Note**
>
> Les définitions de l'état des fonctions d'événement diffèrent légèrement selon les SnapStartfonctions. Pour plus d'informations, consultez États des fonctions Lambda SnapStart et Event.

Dans de nombreux cas, une table DynamoDB constitue un moyen idéal de conservation d'état entre invocations, car elle fournit un accès aux données à faible latence et peut se mettre à l'échelle avec le service Lambda. Vous pouvez également stocker des données dans Amazon EFS pour Lambda si vous utilisez ce service, ce qui permet un accès à faible latence au stockage du système de fichiers.

Les états de la fonction d'événement incluent :

- `Pending` : une fois que Lambda crée la fonction, il définit l'état comme « en attente ». Lorsqu'elle est en attente, Lambda tente de créer ou de configurer des ressources pour la fonction, telles que des ressources VPC ou EFS. Lambda n'appelle pas de fonction pendant que l'état est en attente. Toutes les invocations ou autres actions d'API qui agissent sur la fonction échouent.
- `Active` – La fonction passera à l'état actif lorsque Lambda aura terminé la configuration et l'approvisionnement des ressources. Les fonctions d'événement ne peuvent être invoquées avec succès que lorsqu'elles sont actives.
- `Failed` : indique que la configuration ou l'approvisionnement des ressources ont rencontré une erreur. Lorsque la création d'une fonction échoue, Lambda définit l'état de la fonction sur Echec, et vous devez supprimer et recréer la fonction.
- `Inactive` : une fonction devient inactive lorsqu'elle a été inactive suffisamment longtemps afin que Lambda puisse récupérer les ressources externes qui ont été configurées pour elle. Lorsque vous essayez d'appeler une fonction qui est inactive, l'invocation échoue et Lambda définit la fonction à l'état « en attente » jusqu'à ce que les ressources de la fonction soient recréées. Si

Lambda ne parvient pas à recréer les ressources, la fonction retourne à l'état inactif. Il se peut que vous deviez résoudre les erreurs et redéployer votre fonction pour la rétablir à l'état actif.

Une fonction passe également à l'`Inactive`état si Lambda perd l'accès à l'artefact source de la fonction. Cela s'applique aux fonctions d'image de conteneur dans lesquelles l'image est supprimée d'Amazon ECR ou les autorisations sont révoquées, ainsi qu'aux fonctions .zip qui utilisent un stockage de code S3 autogéré dans lequel l'objet source est supprimé ou les autorisations liées à la politique des compartiments sont révoquées. Pour restaurer la fonction, rétablissez l'accès à l'artefact source et mettez à jour la fonction.

Si vous utilisez des flux de travail SDK-based automatisés ou si vous appelez directement les API de service de Lambda, assurez-vous de vérifier l'état d'une fonction avant de l'appeler pour vérifier qu'elle est active. Vous pouvez le faire à l'aide de l'action GetFunctionde l'API Lambda ou en configurant un serveur à l'aide du SDK pour AWS Java 2.0.

```
aws lambda get-function --function-name my-function --query 'Configuration.[State,
 LastUpdateStatus]'
```

Vous devriez voir la sortie suivante :

```
[
 "Active",
 "Successful"
]
```

Les opérations suivantes échouent lorsque la création de fonction est en attente :

- Invoke
- UpdateFunctionCode
- UpdateFunctionConfiguration
- PublishVersion

États de la fonction d'événement pendant les mises à jour

Lambda effectue deux opérations pour mettre à jour les fonctions d'événement :

- UpdateFunctionCode: met à jour le package de déploiement de la fonction

- UpdateFunctionConfiguration: met à jour la configuration de la fonction

Lambda utilise LastUpdateStatuscet attribut pour suivre la progression de ces opérations de mise à jour. Quand une mise à jour est en cours (`"LastUpdateStatus": "InProgress"`) :

- L'État de la fonction reste `Active`.
- Les invocations continuent d'utiliser le code et la configuration précédents de la fonction jusqu'à ce que la mise à jour soit terminée.
- Les opérations suivantes échouent :
  - UpdateFunctionCode
  - UpdateFunctionConfiguration
  - PublishVersion
  - TagResource

En cas d'échec d'une mise à jour (quand`"LastUpdateStatus": "Failed"`) :

- L'État de la fonction reste `Active`.
- Les invocations continuent d'utiliser le code et la configuration précédents de la fonction.

Example GetFunctionConfiguration réponse

L'exemple suivant est le résultat d'une GetFunctionConfigurationdemande sur une fonction en cours de mise à jour.

```
{
    "FunctionName": "my-function",
    "FunctionArn": "arn:aws:lambda:us-east-1:123456789012:function:my-function",
    "Runtime": "nodejs24.x",
    "VpcConfig": {
        "SubnetIds": [
            "subnet-071f712345678e7c8",
            "subnet-07fd123456788a036",
            "subnet-0804f77612345cacf"
        ],
        "SecurityGroupIds": [
            "sg-085912345678492fb"
        ],
        "VpcId": "vpc-08e1234569e011e83"
```

```
    },
    "State": "Active",
    "LastUpdateStatus": "InProgress",
    ...
}
```

Comprendre le comportement des nouvelles tentatives dans les fonctions d'événement Lambda

Lorsque vous invoquez directement une fonction d'événement, vous déterminez la stratégie de gestion des erreurs liées au code de votre fonction. Lambda ne réessaie pas automatiquement ce type d'erreur en votre nom. Pour réessayer, vous pouvez manuellement invoquer à nouveau votre fonction, envoyer l'événement échoué à une file d'attente pour le débogage, ou ignorer l'erreur. Le code de votre fonction peut s'exécuter entièrement, partiellement ou pas du tout. Si vous recommencez, assurez-vous que le code de votre fonction peut gérer le même événement plusieurs fois, sans provoquer des transactions en double ou d'autres effets secondaires.

Lorsque vous appelez une fonction indirectement, vous devez connaître le comportement de la nouvelle tentative de l'appelant et tout service que la demande rencontre sur le chemin. Cela inclut les scénarios suivants.

- Appel asynchrone – Lambda réessaie deux fois les erreurs de fonction. Si la fonction ne dispose pas de la capacité suffisante pour gérer toutes les requêtes entrantes, des événements peuvent attendre dans la file d'attente pendant des heures ou des jours avant d'être envoyés à la fonction. Vous pouvez configurer une file d'attente de lettres mortes sur la fonction pour capturer les événements qui n'ont pas été traitées avec succès. Pour plus d'informations, consultez the section called “Dead-letter files d'attente”.
- Mappages de source d'événement – Les mappages de source d'événement qui lisent à partir de flux réessaient la totalité du lot d'événements. Les erreurs répétées bloquent le traitement de la partition concernée jusqu'à la résolution de l'erreur ou l'expiration des éléments. Pour détecter des partitions bloquées, vous pouvez surveiller la métrique Âge de l'itérateur.

  Pour les mappages de source d'événement qui lisent à partir d'une file d'attente, vous devez déterminer l'intervalle entre les nouvelles tentatives et la destination pour les événements ayant échoué, en configurant le délai de visibilité et la stratégie de redirection dans la file d'attente source. Pour plus d'informations, consultez Procédure de traitement par Lambda des enregistrements provenant de sources d'événements basées sur des flux et des files d'attente ainsi que les rubriques spécifiques du service dans Invoquer Lambda avec des événements provenant d'autres AWS services.
- AWS services — AWS les services peuvent appeler votre fonction de manière synchrone ou asynchrone. Dans le cas des appels synchrones, le service décide s'il convient d'effectuer une nouvelle tentative. Par exemple, les opérations par lots Amazon S3 réessayent l'opération si la fonction d'événement Lambda renvoie `TemporaryFailure` un code de réponse. Les services qui

demandent par proxy à un utilisateur ou un client en amont peuvent avoir une stratégie de nouvelle tentative ou peuvent transmettre la réponse d'erreur au demandeur. Par exemple, API Gateway transmet toujours la réponse d’erreur au demandeur.

Pour une invocation asynchrone, la logique de nouvelle tentative est la même, quelle que soit la source de l’invocation. Par défaut, Lambda réessaie une invocation asynchrone qui a échoué jusqu’à deux fois. Pour plus d’informations, consultez Méthode de gestion des erreurs et nouvelles tentatives d’invocation asynchrone par Lambda.

- Autres comptes et clients – Lorsque vous accordez l'accès à d'autres comptes, vous pouvez utiliser des stratégies basées sur une ressource afin de restreindre les services ou ressources qu'ils peuvent configurer pour appeler votre fonction. Pour protéger votre fonction de toute surcharge, envisagez de placer une couche d'API devant votre fonction avec Amazon API Gateway. Pour plus d'informations sur la gestion des erreurs d'API Gateway, consultezthe section called “Erreurs”.

Pour vous aider à gérer les erreurs dans les applications Lambda, Lambda s'intègre à des services tels qu'Amazon et. CloudWatch AWS X-Ray Vous pouvez utiliser une combinaison de journaux, de mesures, d'alarmes et de suivi, pour détecter rapidement et d'identifier les problèmes dans le code de votre fonction, de l'API ou d'autres ressources qui prennent en charge votre application. Pour plus d'informations, consultez Surveillance, débogage et résolution des problèmes liés aux fonctions d'événement Lambda.

Utilisation de la détection de boucle récursive Lambda pour prévenir les boucles infinies

Lorsque vous configurez une fonction d'événement Lambda pour qu'elle soit envoyée au même service ou à la même ressource qui invoque la fonction, il est possible de créer une boucle récursive infinie. Par exemple, une fonction d'événement Lambda peut écrire un message dans une file d'attente Amazon Simple Queue Service (Amazon SQS), qui invoque ensuite la même fonction. Cette invocation amène la fonction à écrire un autre message dans la file d'attente, qui à son tour invoque à nouveau la fonction.

Les boucles récursives involontaires peuvent entraîner la facturation de frais imprévus à votre charge. Compte AWS Les boucles peuvent également entraîner la mise à l'échelle de Lambda et l'utilisation de toute la simultanéité disponible de votre compte. Pour réduire l'impact des boucles non intentionnelles, Lambda détecte certains types de boucles récursives peu de temps après leur apparition.

Par défaut, lorsque Lambda détecte une boucle récursive, il arrête l'invocation de votre fonction et vous en informe. Si votre conception utilise intentionnellement des schémas récursifs, vous pouvez modifier la configuration par défaut d'une fonction pour permettre à celle-ci d'être invoquée de manière récursive. Pour plus d'informations, consultez the section called "Autoriser l'exécution d'une fonction d'événement Lambda dans une boucle récursive".

Sections

- Comprendre la détection de boucles récursives
- Pris en charge Services AWS et SDK
- Notifications de boucles récursives
- Répondre aux notifications de détection de boucles récursives
- Autoriser l'exécution d'une fonction d'événement Lambda dans une boucle récursive
- Régions prises en charge pour la détection des boucles récursives de Lambda

Comprendre la détection de boucles récursives

La détection de boucles récursives dans Lambda fonctionne en suivant les événements. Lambda est un service de calcul piloté par les événements qui exécute le code de votre fonction lorsque certains événements se produisent. Par exemple, lorsqu'un élément est ajouté à une file d'attente Amazon SQS ou à une rubrique Amazon Simple Notification Service (Amazon SNS). Lambda transmet les

événements à votre fonction sous forme d'objets JSON, qui contiennent des informations sur la modification d'état du système. Lorsqu'un événement provoque l'exécution de votre fonction, cela s'appelle une invocation.

Pour détecter les boucles récursives, Lambda utilise des en-têtes de suivi AWS X-Ray. Lorsque les Services AWS qui prennent en charge cette la détection des boucles récursives envoient des événements à Lambda, ces événements sont automatiquement annotés avec des métadonnées. Lorsque votre fonction d'événement Lambda écrit l'un de ces événements dans une autre fonction prise en charge à Service AWS l'aide d'une version prise en charge d'un AWS SDK, elle met à jour ces métadonnées. Les métadonnées mises à jour comprennent un décompte du nombre de fois où l'événement a invoqué la fonction.

> **Note**
>
> Il n'est pas nécessaire d'activer le suivi X-Ray actif pour que cette fonctionnalité fonctionne. La détection des boucles récursives est activée par défaut pour tous les clients AWS . L'utilisation de cette fonctionnalité est gratuite.

Une chaîne de requêtes est une séquence d'invocations Lambda provoquée par le même événement déclencheur. Par exemple, imaginez qu'une file d'attente Amazon SQS invoque votre fonction d'événement Lambda. Votre fonction d'événement Lambda renvoie ensuite l'événement traité à la même file d'attente Amazon SQS, qui invoque à nouveau votre fonction. Dans cet exemple, chaque invocation de votre fonction appartient à la même chaîne de requêtes.

Si votre fonction est invoquée environ 16 fois dans la même chaîne de requêtes, Lambda arrête automatiquement l’invocation de fonction suivante dans cette chaîne de requêtes et vous en informe. Si votre fonction est configurée avec plusieurs déclencheurs, les invocations provenant d'autres déclencheurs ne sont pas affectées.

> **Note**
>
> Même lorsque le paramètre `maxReceiveCount` de la politique de redirection de la file d’attente source est supérieur à 16, la protection contre la récursion Lambda n’empêche pas Amazon SQS de réessayer le message après la détection et l’arrêt d’une boucle récursive. Lorsque Lambda détecte une boucle récursive et interrompt les invocations suivantes, il renvoie une `RecursiveInvocationException` au mappage des sources d'événements. Cela augmente la valeur `receiveCount` du message. Lambda continue de réessayer le

message et de bloquer les invocations de fonctions jusqu'à ce qu'Amazon SQS détermine que le délai `maxReceiveCount` est dépassé et envoie le message à la file d'attente de lettres mortes configurée.

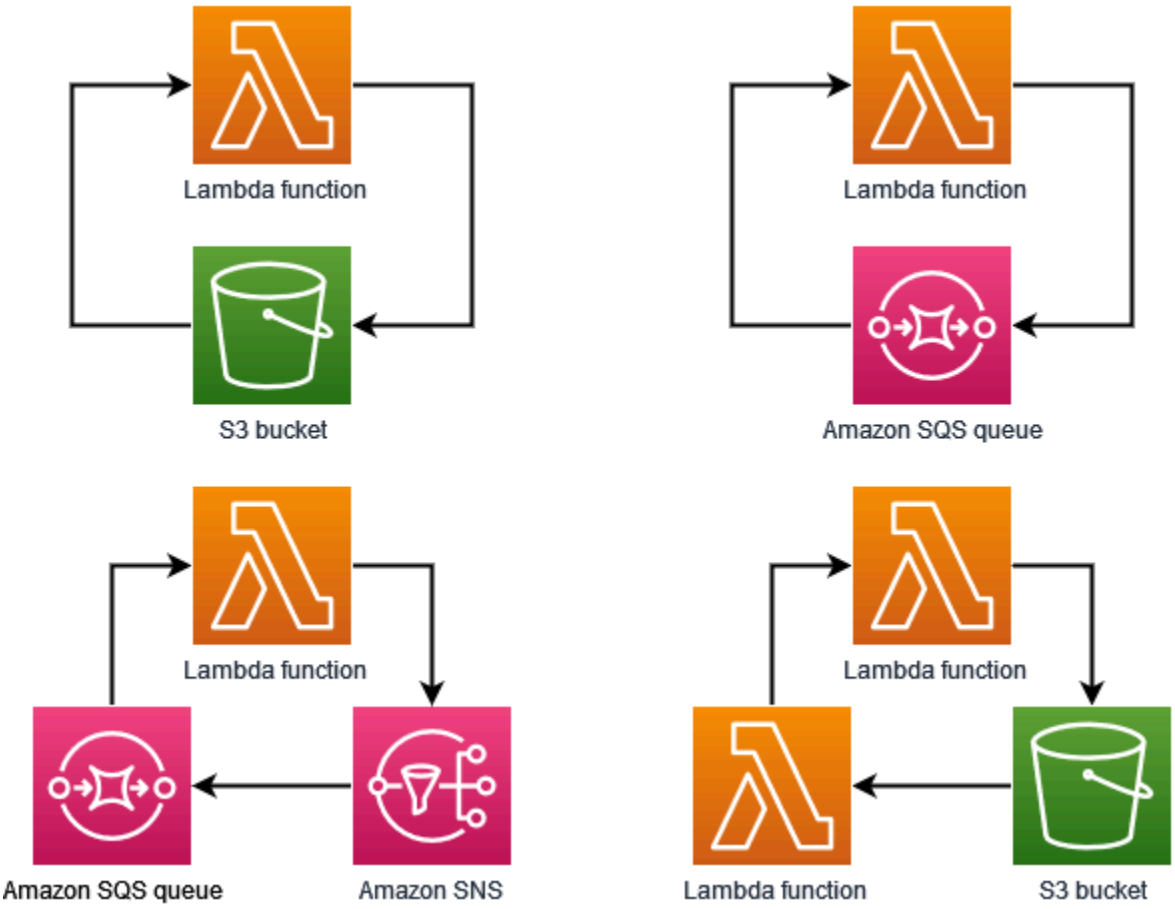
Si vous avez configuré une destination en cas de défaillance ou une file d'attente de lettres mortes pour votre fonction d'événement, Lambda envoie également l'événement depuis l'invocation interrompue vers votre destination ou votre file d'attente de lettres mortes. Lorsque vous configurez une file d'attente de destination ou une file d'attente de lettres mortes pour votre fonction, assurez-vous de ne pas utiliser un déclencheur d'événement ou mappage des sources d'événements que votre fonction utilise également. Si vous envoyez des événements à la même ressource qui appelle votre fonction, vous pouvez créer une autre boucle récursive et cette boucle sera également interrompue. Si vous désactivez la détection des boucles de récursivité, cette boucle n'est pas interrompue.

Pris en charge Services AWS et SDK

Lambda ne peut détecter que les boucles récursives dont certaines sont prises en charge. Services AWS Pour que les boucles récursives soient détectées, votre fonction d'événement doit également utiliser l'un des AWS SDK pris en charge.

Pris en charge Services AWS

Lambda détecte actuellement les boucles récursives entre vos fonctions, Amazon SQS, Amazon S3, Amazon SNS et les bus d'événements Amazon Custom. EventBridge Lambda détecte également les boucles composées uniquement de fonctions d'événement Lambda, qui peuvent s'invoquer mutuellement de manière synchrone ou asynchrone. Les schémas suivants montrent quelques exemples de boucles que Lambda peut détecter :



Lorsqu'une autre Service AWS , telle qu'Amazon DynamoDB, fait partie de la boucle, Lambda ne peut actuellement pas la détecter ni l'arrêter.

Comme Lambda ne détecte actuellement que les boucles récursives impliquant des bus d'événements Amazon SQS, Amazon S3, Amazon SNS et EventBridge Amazon Custom, il est toujours possible que des boucles impliquant Services AWS d'autres bus entraînent une utilisation involontaire de votre fonction d'événement Lambda.

Pour éviter que des frais imprévus ne vous soient facturés Compte AWS, nous vous recommandons de configurer les CloudWatchalarmes Amazon pour vous avertir des habitudes d'utilisation inhabituelles. Par exemple, vous pouvez configurer pour vous CloudWatch avertir des pics de simultanéité ou d'invocation des fonctions d'événement Lambda. Vous pouvez également configurer une alarme de facturation pour vous avertir lorsque les dépenses sur votre compte dépassent un seuil que vous avez spécifié. Vous pouvez également utiliser AWS Cost Anomaly Detectionpour vous alerter en cas de schémas de facturation inhabituels.

Pris en charge AWS Kits SDK

Pour que Lambda détecte les boucles récursives, votre fonction doit utiliser l'une des versions suivantes ou plus récentes du kit SDK :

Environnement d’exécution	Version minimale du AWS SDK requise
Node.js	2.1147.0 (kit SDK version 2) 3.105.0 (kit SDK version 3)
Python	1.24.46 (boto3) 1.27.46 (botocore)
Java 8 et Java 11	2,17135
Java 17	2,20,81
Java 21	2,21,24
.NET	3,7,293,0
Ruby	3,134,0
PHP	3,232,0
Go	SDK V2 1.57.0

Certains environnements d'exécution Lambda, tels que Python, Node.js incluent une version du SDK. AWS Si la version du kit SDK incluse dans l'exécution de votre fonction est inférieure au minimum requis, vous pouvez ajouter une version prise en charge du kit SDK au package de déploiement de votre fonction. Vous pouvez également ajouter une version du kit SDK compatible à votre fonction à l'aide d'une couche Lambda. Pour obtenir la liste des kits SDK inclus dans chaque exécution Lambda, consultez Exécutions de la fonction Lambda Event.

Notifications de boucles récursives

Lorsque Lambda arrête une boucle récursive, vous recevez des notifications le Tableau de bord Health et par e-mail. Vous pouvez également utiliser CloudWatch des métriques pour surveiller le nombre d'appels récursifs interrompus par Lambda.

Tableau de bord Health notifications

Lorsque Lambda arrête un appel récursif, une notification s' Tableau de bord Health affiche sur la page de santé de votre compte, sous Problèmes ouverts et récents. Notez qu'il peut s'écouler jusqu'à trois heures et demie après l'arrêt d'une invocation récursive par Lambda avant que cette notification ne s'affiche. Pour plus d'informations sur l'affichage des événements du compte dans le Tableau de bord Health, consultez Getting started with your AWS Health Dashboard — Your account health dans le AWS Health User Guide.

Alertes par e-mail

Lorsque Lambda arrête pour la première fois un appel récursif de votre fonction d'événement, il vous envoie une alerte par e-mail. Lambda envoie au maximum un e-mail toutes les 24 heures pour chaque fonction de votre Compte AWS. Une fois que Lambda a envoyé une notification par e-mail, vous ne recevrez plus d'e-mails pour cette fonction pendant 24 heures, même si Lambda arrête d'autres invocations récursives de la fonction. Notez qu'il peut s'écouler jusqu'à trois heures et demie après l'arrêt d'une invocation récursive par Lambda avant que vous ne receviez cette alerte par e-mail.

Lambda envoie des alertes par e-mail en boucle récursive au contact principal Compte AWS de votre compte et au contact opérationnel alternatif. Pour plus d'informations sur l'affichage ou la mise à jour des adresses e-mail de votre compte, consultez la section Mise à jour des informations de contact dans la Référence générale AWS .

CloudWatch Métriques Amazon

La CloudWatch métrique `RecursiveInvocationsDropped` enregistre le nombre d'invocations de fonctions que Lambda a arrêtées parce que votre fonction a été invoquée plus de 16 fois environ au cours d'une même chaîne de requêtes. Lambda émet cette métrique dès qu'il arrête une invocation récursive. Pour afficher cette métrique, suivez les instructions relatives à l'affichage des métriques sur la CloudWatch console et choisissez la métrique`RecursiveInvocationsDropped`.

Répondre aux notifications de détection de boucles récursives

Lorsque votre fonction d'événement est invoquée plus de 16 fois environ par le même événement déclencheur, Lambda arrête l'appel de fonction suivant pour cet événement afin de rompre la boucle récursive. Pour éviter qu'une boucle récursive interrompue par Lambda ne se reproduise, procédez comme suit :

- Réduisez la simultanéité disponible de votre fonction à zéro, ce qui limite toutes les invocations futures.
- Supprimez ou désactivez le déclencheur ou le mappage des sources d'événements qui invoque votre fonction.
- Identifiez et corrigez les défauts de code qui réécrivent les événements dans la AWS ressource qui appelle votre fonction. Une source fréquente de défauts survient lorsque vous utilisez des variables pour définir la source et la cible des événements d'une fonction. Vérifiez que vous n'utilisez pas la même valeur pour les deux variables.

En outre, si la source d'événement de votre fonction d'événement Lambda est une file d'attente Amazon SQS, envisagez de configurer une file d'attente de lettres mortes dans la file d'attente source.

> **Note**
>
> Assurez-vous de configurer la file d'attente contenant des lettres mortes sur la file d'attente source, et non sur la fonction d'événement Lambda. La file d’attente de lettres mortes que vous configurez dans une fonction est utilisée pour la file d’attente d’invocation asynchrone et non pour les files d’attente source d’événement.

Si la source de l'événement est une rubrique Amazon SNS, pensez à ajouter une destination en cas d'échec pour votre fonction.

Pour réduire à zéro la simultanéité disponible de votre fonction événementielle (console)

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez le nom de votre fonction événementielle.
3. Choisissez Limiter.
4. Dans la boîte de dialogue Limiter votre fonction, choisissez Confirmer.

Pour supprimer un déclencheur ou un mappage de source d'événement pour votre fonction d'événement (console)

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez le nom de votre fonction événementielle.
3. Choisissez l'onglet Configuration, puis Déclencheurs.
4. Sous Déclencheurs, sélectionnez le déclencheur ou le mappage des sources d'événements que vous souhaitez supprimer, puis choisissez Supprimer.
5. Dans la boîte de dialogue Supprimer des déclencheurs, choisissez Supprimer.

Pour désactiver le mappage d'une source d'événement pour votre fonction d'événement (AWS CLI)

1. Pour trouver l'UUID du mappage des sources d'événements que vous souhaitez désactiver, exécutez la commande AWS Command Line Interface (AWS CLI) list-event-source-mappings.

```
aws lambda list-event-source-mappings
```

2. Pour désactiver le mappage des sources d'événements, exécutez la commande AWS CLI update-event-source-mapping suivante.

```
aws lambda update-event-source-mapping --function-name MyFunction \
--uuid a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 --no-enabled
```

Autoriser l'exécution d'une fonction d'événement Lambda dans une boucle récursive

Si votre conception utilise intentionnellement une boucle récursive, vous pouvez configurer une fonction d'événement Lambda pour permettre son appel récursif. Nous vous recommandons d'éviter d'utiliser des boucles récursives dans votre conception. Les erreurs de mise en œuvre peuvent entraîner des appels récursifs utilisant toutes les données disponibles simultanément et des frais imprévus facturés sur votre Compte AWS compte.

> **Important**
>
> Si vous utilisez des boucles récursives, traitez-les avec prudence. Mettez en œuvre des barrières de protection conformes aux pratiques exemplaires afin de minimiser les risques d'erreurs de mise en œuvre. Pour en savoir plus sur les pratiques exemplaires en matière

d'utilisation de modèles d'invocation récursifs, consultez Recursive patterns that cause run-away Lambda functions sur Serverless Land.

Vous pouvez configurer des fonctions pour autoriser les boucles récursives à l'aide de la console Lambda, AWS Command Line Interface du AWS CLI() et PutFunctionRecursionConfigde l'API. Vous pouvez également configurer le paramètre de détection de boucle récursive d'une fonction dans AWS SAM et CloudFormation.

Par défaut, Lambda détecte et arrête les boucles récursives. À moins que votre conception n'utilise intentionnellement une boucle récursive, nous vous recommandons de ne pas modifier la configuration par défaut de vos fonctions.

Notez que lorsque vous configurez une fonction pour autoriser les boucles récursives, la CloudWatch métrique `RecursiveInvocationsDropped` n'est pas émise.

Console

Pour autoriser l'exécution d'une fonction d'événement dans une boucle récursive (console)

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez le nom de votre fonction événementielle pour ouvrir la page détaillée de la fonction.
3. Choisissez l'onglet Configuration, puis sélectionnez Concurrence et détection de récursivité.
4. En regard de Détection de boucle récursive, choisissez Modifier.
5. Sélectionnez Autoriser les boucles récursives.
6. Cliquez sur Enregistrer.

AWS CLI

Vous pouvez utiliser l'PutFunctionRecursionConfigAPI pour permettre à votre fonction d'être invoquée dans une boucle récursive. Spécifiez `Allow` pour le paramètre de boucle récursive. Par exemple, vous pouvez appeler cette API avec la `put-function-recursion-config` AWS CLI commande suivante :

```
aws lambda put-function-recursion-config --function-name yourFunctionName --
recursive-loop Allow
```

Vous pouvez rétablir la configuration par défaut de votre fonction d'événement afin que Lambda mette fin aux boucles récursives lorsqu'il les détecte. Modifiez la configuration de votre fonction à l'aide de la console Lambda ou de l' AWS CLI.

Console

Pour configurer une fonction d'événement afin de mettre fin aux boucles récursives (console)

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez le nom de votre fonction événementielle pour ouvrir la page détaillée de la fonction.
3. Choisissez l'onglet Configuration, puis sélectionnez Concurrence et détection de récursivité.
4. En regard de Détection de boucle récursive, choisissez Modifier.
5. Sélectionnez Mettre fin aux boucles récursives.
6. Cliquez sur Enregistrer.

AWS CLI

Vous pouvez utiliser l'PutFunctionRecursionConfigAPI pour configurer votre fonction afin que Lambda mette fin aux boucles récursives lorsqu'il les détecte. Spécifiez `Terminate` pour le paramètre de boucle récursive. Par exemple, vous pouvez appeler cette API avec la `put-function-recursion-config` AWS CLI commande suivante :

```
aws lambda put-function-recursion-config --function-name yourFunctionName --
recursive-loop Terminate
```

Régions prises en charge pour la détection des boucles récursives de Lambda

La détection par boucle récursive Lambda est prise en charge dans toutes les régions commerciales.

Création et gestion des URL de fonctions Lambda

L'URL d'une fonction est un point de terminaison HTTP (S) dédié à votre fonction d'événement Lambda. Vous pouvez créer et configurer une URL de fonction via la console Lambda ou l'API Lambda.

> **Tip**
>
> Lambda propose deux méthodes pour invoquer votre fonction via un point de terminaison HTTP : les URL de fonction et Amazon API Gateway. Si vous ne savez pas quelle est la meilleure méthode pour votre cas d'utilisation, consultez the section called "URL de fonction et Amazon API Gateway".

Lorsque vous créez une URL de fonction, Lambda génère automatiquement un point de terminaison URL unique pour vous. Une fois que vous avez créé une URL de fonction, son point de terminaison URL ne change jamais. Les points de terminaison URL de fonction ont le format suivant :

```
https://<url-id>.lambda-url.<region>.on.aws
```

> **Note**
>
> Les URL des fonctions ne sont pas prises en charge dans toutes les AWS régions. Pour vérifier la disponibilité, consultez la section Services AWS régionaux et filtrez par`Feature Name = Function URLs`.

Les URL de fonctions sont compatibles avec la pile double, prenant en charge les adresses IPv4 et IPv6. Après avoir configuré une URL de fonction pour votre fonction, vous pouvez appeler votre fonction via son point de terminaison HTTP (S) à l'aide d'un navigateur Web, d'un curl, de Postman ou de tout autre client HTTP.

> **Note**
>
> Vous pouvez accéder à l'URL de votre fonction via l'Internet public uniquement. Bien que les fonctions d'événement Lambda soient prises en charge AWS PrivateLink, les URL des fonctions ne le sont pas.

Les URL de fonctions Lambda utilisent des stratégies basées sur les ressources pour la sécurité et le contrôle d'accès. Les URL de fonctions prennent également en charge les options de configuration du partage des ressources cross-origin (CORS).

Vous pouvez appliquer des URL de fonctions à n'importe quel alias de fonction ou à la version non publiée `$LATEST` de la fonction. Vous ne pouvez pas ajouter d'URL de fonction à une autre version de fonction.

La section suivante explique comment créer et gérer une URL de fonction à l'aide de la console Lambda et CloudFormation du AWS CLI modèle. Pour un didacticiel étape par étape sur l'utilisation des URL de fonctions comme points de terminaison de webhook, voir. the section called "Didacticiel : création d'un point de terminaison de webhook"

Rubriques

- Création d'une URL de fonction (console)
- Création d'une URL de fonction (AWS CLI)
- Ajouter l'URL d'une fonction à un CloudFormation modèle
- Cross-origin partage de ressources (CORS)
- Limitation des URL de fonctions
- Désactivation des URL de fonctions
- Suppression d'URL de fonction
- Contrôle d'accès aux URL de fonctions Lambda
- Invocation d'URL de fonctions Lambda
- Surveillance des URL de fonctions Lambda
- Sélectionnez une méthode pour appeler votre fonction d'événement Lambda à l'aide d'une requête HTTP
- Didacticiel : création d'un point de terminaison webhook à l'aide d'une URL de fonction Lambda

Création d'une URL de fonction (console)

Suivez ces étapes pour créer une URL de fonction à l'aide de la console.

Créer une URL de fonction pour une fonction existante

1. Ouvrez la page Event Functions de la console Lambda.

2. Choisissez le nom de la fonction d'événement pour laquelle vous souhaitez créer l'URL de la fonction.
3. Choisissez l'onglet Configuration, puis Function URL (URL de fonction).
4. Choisissez Create function URL (Créer une URL de fonction).
5. Pour Auth type (type d'authentification), choisissez AWS_IAM ou NONE(AUCUN). Pour plus d'informations sur l'authentification de l'URL de fonction, consultez Contrôle d'accès.
6. (Facultatif) Sélectionnez Configure cross-origin resource sharing (CORS) (Configurer le partage des ressources cross-origin [CORS]), puis configurez les paramètres CORS pour l'URL de votre fonction. Pour plus d'informations sur le CORS, consultez Cross-origin partage de ressources (CORS).
7. Choisissez Save (Enregistrer).

Une URL de fonction est créée pour la version non publiée `$LATEST` de votre fonction. L'URL de la fonction s'affiche dans la section Function overview (Présentation de la fonction) de la console.

Créer une URL de fonction pour un alias existant

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez le nom de la fonction d'événement avec l'alias pour lequel vous souhaitez créer l'URL de la fonction.
3. Choisissez l'onglet Aliases (Alias), puis le nom de l'alias pour lequel vous souhaitez créer l'URL de fonction.
4. Choisissez l'onglet Configuration, puis Function URL (URL de fonction).
5. Choisissez Create function URL (Créer une URL de fonction).
6. Pour Auth type (type d'authentification), choisissez AWS_IAM ou NONE(AUCUN). Pour plus d'informations sur l'authentification de l'URL de fonction, consultez Contrôle d'accès.
7. (Facultatif) Sélectionnez Configure cross-origin resource sharing (CORS) (Configurer le partage des ressources cross-origin [CORS]), puis configurez les paramètres CORS pour l'URL de votre fonction. Pour plus d'informations sur le CORS, consultez Cross-origin partage de ressources (CORS).
8. Cliquez sur Enregistrer.

Cela crée une URL de fonction pour votre alias de fonction. L'URL de fonction s'affiche dans la section Function overview (Présentation des fonctions) de la console.

Créer une nouvelle fonction avec une URL de fonction

Pour créer une nouvelle fonction d'événement avec une URL de fonction (console)

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez Create Event Function.
3. Sous Basic information (Informations de base), procédez comme suit :
   a. Dans Function name (nom de la fonction), saisissez un nom pour votre fonction, par exemple **`my-function`**.
   b. Pour Runtime, choisissez le langage d'exécution que vous préférez, par exemple Node.js 24.
   c. Pour Architecture, choisissez x86_64 ou arm64.
   d. Développez Permissions (Autorisations), puis choisissez si vous souhaitez créer un nouveau rôle d'exécution ou utiliser un rôle existant.
4. Développez Advanced settings (Paramètres avancés), puis sélectionnez Function URL (URL de fonction).
5. Pour Auth type (type d'authentification), choisissez AWS_IAM ou NONE(AUCUN). Pour plus d'informations sur l'authentification de l'URL de fonction, consultez Contrôle d'accès.
6. (Facultatif) Sélectionnez Configure cross-origin resource sharing (CORS) (Configuration du partage des ressources cross-origin). En sélectionnant cette option lors de la création de la fonction, l'URL de votre fonction autorise par défaut les demandes de toutes les origines. Vous pouvez modifier les paramètres CORS de l'URL de votre fonction après avoir créé la fonction. Pour plus d'informations sur le CORS, consultez Cross-origin partage de ressources (CORS).
7. Choisissez Create Event Function.

Ceci crée une nouvelle fonction avec une URL de fonction pour la `$LATEST` version non publiée de la fonction. L'URL de la fonction s'affiche dans la section Function overview (Présentation des fonctions) de la console.

Création d'une URL de fonction (AWS CLI)

Pour créer une URL de fonction pour une fonction d'événement Lambda existante à l'aide de AWS Command Line Interface (AWS CLI), exécutez la commande suivante :

```
aws lambda create-function-url-config \
```

```
    --function-name my-function \
    --qualifier prod \ // optional
    --auth-type AWS_IAM
    --cors-config {AllowOrigins="https://example.com"} // optional
```

Une URL de fonction est ajoutée au qualificateur **`prod`** pour la fonction **`my-function`**. Pour plus d'informations sur ces paramètres de configuration, consultez CreateFunctionUrlConfig dans la référence d'API.

> **Note**
>
> Pour créer une URL de fonction à l'aide de AWS CLI, la fonction doit déjà exister.

Ajouter l'URL d'une fonction à un CloudFormation modèle

Pour ajouter une `AWS::Lambda::Url` ressource à votre CloudFormation modèle, utilisez la syntaxe suivante :

JSON

```
{
  "Type" : "AWS::Lambda::Url",
  "Properties" : {
      "AuthType" : String,
      "Cors" : Cors,
      "Qualifier" : String,
      "TargetFunctionArn" : String
    }
}
```

YAML

```
Type: AWS::Lambda::Url
Properties:
  AuthType: String
  Cors:
    Cors
  Qualifier: String
  TargetFunctionArn: String
```

Parameters

- (Obligatoire) `AuthType` – Définit le type d'authentification pour l'URL de votre fonction. Les valeurs possibles sont soit `AWS_IAM`, soit `NONE`. Pour limiter l'accès aux utilisateurs authentifiés uniquement, définissez la valeur sur `AWS_IAM`. Pour contourner l'authentification IAM et autoriser n'importe quel utilisateur à envoyer des demandes à votre fonction, définissez la valeur `NONE`.
- (Facultatif) `Cors` – Définit les paramètres CORS de l'URL de votre fonction. Pour ajouter `Cors` des éléments à votre `AWS::Lambda::Url` ressource CloudFormation, utilisez la syntaxe suivante.

  Example AWS::Lambda : : Url.Cors (JSON)

  ```
  {
    "AllowCredentials" : Boolean,
    "AllowHeaders" : [ String, ... ],
    "AllowMethods" : [ String, ... ],
    "AllowOrigins" : [ String, ... ],
    "ExposeHeaders" : [ String, ... ],
    "MaxAge" : Integer
  }
  ```

  Example AWS::Lambda : : Url.Cors (YAML)

  ```
    AllowCredentials: Boolean
    AllowHeaders:
      - String
    AllowMethods:
      - String
    AllowOrigins:
      - String
    ExposeHeaders:
      - String
    MaxAge: Integer
  ```

- (Facultatif) `Qualifier` – Le nom de l'alias.
- (Obligatoire) `TargetFunctionArn` — Le nom ou le nom de ressource Amazon (ARN) de la fonction d'événement Lambda. Les formats de nom valides sont notamment les suivants :
  - Nom de fonction – `my-function`
  - ARN de fonction – `arn:aws:lambda:us-west-2:123456789012:function:my-function`

- ARN partiel – `123456789012:function:my-function`

Cross-origin partage de ressources (CORS)

Pour définir comment différentes origines peuvent accéder à l'URL de votre fonction, utilisez le partage de ressources cross-origin (CORS). Nous vous recommandons de configurer CORS si vous avez l'intention d'appeler l'URL de votre fonction à partir d'un autre domaine. Lambda prend en charge les en-têtes CORS suivants pour les URL de fonctions.

En-têtes CORS	Propriété de configuration CORS	Exemples de valeur

Access-Control-Allow-Origin	`AllowOrigins`	`*` (autoriser toutes les origines)
		`https://www.example.com`
		`http://localhost:60905`

Access-Control-Allow-Methods	`AllowMethods`	`GET`, `POST`, `DELETE`, `*`
Access-Control-Allow-Headers	`AllowHeaders`	`Date`, `Keep-Alive` , `X-Custom-Header`
Access-Control-Expose-Headers	`ExposeHeaders`	`Date`, `Keep-Alive` , `X-Custom-Header`
Access-Control-Allow-Credentials	`AllowCredentials`	`TRUE`
Access-Control-Max-Age	`MaxAge`	`5` (par défaut), `300`

Lorsque vous configurez CORS pour une URL de fonction à l'aide de la console Lambda ou du AWS CLI, Lambda ajoute automatiquement les en-têtes CORS à toutes les réponses via l'URL de la fonction. Vous pouvez également ajouter manuellement des en-têtes CORS à la réponse de votre fonction. En cas de conflit d'en-têtes, le comportement attendu dépend du type de la requête :

- Pour les requêtes en amont, telles que les requêtes OPTIONS, les en-têtes CORS configurés sur l'URL de la fonction ont priorité. Lambda renvoie uniquement ces en-têtes CORS dans la réponse.
- Pour les requêtes autres que celles effectuées en amont, telles que les requêtes GET ou POST, Lambda renvoie à la fois les en-têtes CORS configurés sur l'URL de la fonction, ainsi que les en-têtes CORS renvoyés par la fonction. Cela peut entraîner une duplication d'en-têtes CORS dans la réponse. Vous pouvez voir une erreur similaire à ce qui suit : `The 'Access-Control-Allow-Origin' header contains multiple values '*, *', but only one is allowed`.

En général, nous recommandons de configurer tous les paramètres CORS sur l'URL de la fonction, plutôt que d'envoyer les en-têtes CORS manuellement dans la réponse de la fonction.

Limitation des URL de fonctions

La limitation limite le débit auquel la fonction traite les demandes. Cette fonction est utile dans de nombreuses situations, notamment pour empêcher votre fonction de surcharger les ressources en aval ou pour gérer une augmentation soudaine des demandes.

Vous pouvez limiter le taux de requêtes traitées par votre fonction d'événement Lambda via une URL de fonction en configurant la simultanéité réservée. La simultanéité réservée limite le nombre maximal d'invocations simultanées pour votre fonction. Le débit de demandes maximal par seconde (RPS) de votre fonction est équivalent à 10 fois la simultanéité réservée configurée. Par exemple, si vous configurez votre fonction avec une simultanéité réservée de 100, le RPS maximal est de 1 000.

Lorsque la simultanéité de la fonction dépasse la simultanéité réservée, l'URL de votre fonction renvoie un code d'état HTTP 429. Si votre fonction reçoit une demande qui dépasse le maximum de 10 fois le RPS par rapport à la simultanéité réservée configurée, vous recevez également une erreur HTTP 429. Pour de plus amples informations sur la simultanéité réservée, consultez Configuration de la simultanéité réservée pour une fonction événementielle.

Désactivation des URL de fonctions

En cas d'urgence, vous pouvez rejeter tout le trafic vers l'URL de fonction. Pour désactiver votre URL de fonction, définissez la simultanéité réservée sur zéro. Cela limite toutes les demandes envoyées à l'URL de votre fonction, ce qui entraîne des réponses d'état HTTP 429. Pour réactiver l'URL de votre fonction, supprimez la configuration de simultanéité réservée ou définissez la configuration sur un montant supérieur à zéro.

Suppression d'URL de fonction

Lorsque vous supprimez une URL de fonction, vous ne pouvez pas la récupérer. La création d'une nouvelle URL de fonction génère une adresse URL différente.

> **Note**
>
> Si vous supprimez une URL de fonction avec un type d'authentification `NONE`, Lambda ne supprime pas automatiquement la politique basée sur les ressources associée. Si vous souhaitez supprimer cette politique, vous devez le faire manuellement.

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez le nom de la fonction d'événement.
3. Choisissez l'onglet Configuration, puis Function URL (URL de fonction).
4. Sélectionnez Delete (Supprimer).
5. Entrez le mot delete dans le champ pour confirmer la suppression.
6. Sélectionnez Supprimer.

> **Note**
>
> Lorsque vous supprimez une fonction qui possède une URL de fonction, Lambda supprime cette URL de manière asynchrone. Si vous créez immédiatement une nouvelle fonction portant le même nom dans le même compte, il est possible que l'URL de la fonction d'origine soit mappée à la nouvelle fonction au lieu d'être supprimée.

Contrôle d'accès aux URL de fonctions Lambda

> **Note**
>
> À compter d'octobre 2025, les nouvelles URL de fonction nécessiteront à la fois les autorisations `lambda:InvokeFunctionUrl` et `lambda:InvokeFunction`.

Vous pouvez contrôler l'accès aux URL de vos fonctions Lambda à l'aide du AuthTypeparamètre combiné aux politiques basées sur les ressources associées à votre fonction d'événement spécifique.

La configuration de ces deux composants détermine qui peut invoquer ou exécuter d'autres actions administratives sur l'URL de votre fonction.

Le paramètre `AuthType` détermine comment Lambda authentifie ou autorise les demandes vers l'URL de votre fonction. Lorsque vous configurez l'URL de votre fonction, vous devez spécifier l'une des options `AuthType` suivantes :

- `AWS_IAM`— Lambda utilise Gestion des identités et des accès AWS (IAM) pour authentifier et autoriser les demandes en fonction de la politique d'identité du principal IAM et de la politique basée sur les ressources de la fonction. Choisissez cette option si vous souhaitez que seuls les utilisateurs et les rôles authentifiés invoquent votre fonction via l'URL de la fonction.

- `NONE` – Lambda n'effectue aucune authentification avant d'invoquer votre fonction. Toutefois, la stratégie basée sur les ressources de votre fonction est toujours en vigueur et doit accorder un accès public avant que l'URL de votre fonction puisse recevoir des demandes. Choisissez cette option pour autoriser un accès public et non authentifié à l'URL de votre fonction.

Pour obtenir des informations supplémentaires sur la sécurité, vous pouvez AWS Identity and Access Management Access Analyzer obtenir une analyse complète de l'accès externe à l'URL de votre fonction. IAM Access Analyzer surveille également les autorisations nouvelles ou mises à jour sur vos fonctions d'événement Lambda afin de vous aider à identifier les autorisations qui accordent un accès public et entre comptes. Vous pouvez utiliser IAM Access Analyzer sans frais. Pour démarrer avec IAM Access Analyzer, consultez Utilisation d' AWS IAM Access Analyzer.

Cette page contient des exemples de politiques basées sur les ressources pour les deux types d'authentification et explique comment créer ces politiques à l'aide de l'opération AddPermissionAPI ou de la console Lambda. Pour plus d'informations sur la procédure d'invocation de l'URL de votre fonction après avoir configuré les autorisations, consultez Invocation d'URL de fonctions Lambda.

Rubriques

- Utilisation du type d'authentification AWS_IAM
- Utilisation du type d'authentification NONE
- Gouvernance et contrôle d'accès

Utilisation du type d'authentification **`AWS_IAM`**

Si vous choisissez le type d'authentification `AWS_IAM`, les utilisateurs qui ont besoin d'invoquer l'URL de votre fonction Lambda doivent avoir les autorisations `lambda:InvokeFunctionUrl` et `lambda:InvokeFunction`. Selon la personne qui effectue la demande d'invocation, vous devrez peut-être accorder cette autorisation à l'aide d'une stratégie basée sur les ressources.

Si le principal qui fait la demande se trouve dans la même URL Compte AWS que l'URL de la fonction, il doit soit disposer `lambda:InvokeFunctionUrl` d'`lambda:InvokeFunction`autorisations dans sa politique basée sur l'identité, soit avoir des autorisations qui lui sont accordées dans le cadre de la politique basée sur les ressources de la fonction. En d'autres termes, une stratégie basée sur les ressources est facultative si l'utilisateur possède déjà des autorisations `lambda:InvokeFunctionUrl` et `lambda:InvokeFunction` dans sa stratégie basée sur l'identité. L'évaluation des politiques suit les règles décrites dans la Logique d'évaluation des politiques.

Si le principal qui fait la demande se trouve dans un autre compte, il doit avoir à la fois une stratégie basée sur l'identité qui lui donne des autorisations `lambda:InvokeFunctionUrl` et `lambda:InvokeFunction`, et des autorisations qui lui sont accordées dans une stratégie basée sur les ressources de la fonction qu'il essaie d'invoquer. L'évaluation des stratégies suit les règles décrites dans Comment déterminer si une demande d'accès entre comptes est autorisée.

La politique basée sur les ressources suivante permet au `example` rôle in d'invoquer l'URL Compte AWS `444455556666` de la fonction associée à la fonction. `my-function` La touche de InvokedViaFunctionUrl contexte lambda : limite l'`lambda:InvokeFunction`action aux appels d'URL de fonction. Cela signifie que le principal doit utiliser l'URL de la fonction pour invoquer la fonction. Si vous n'incluez pas `lambda:InvokedViaFunctionUrl`, le principal peut invoquer votre fonction via d'autres méthodes d'invocation, en plus de l'URL de la fonction.

Example— politique Cross-account basée sur les ressources

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::444455556666:role/example"
```

```
      },
      "Action": "lambda:InvokeFunctionUrl",
      "Resource": "arn:aws:lambda:us-east-1:123456789012:function:my-function",
      "Condition": {
        "StringEquals": {
          "lambda:FunctionUrlAuthType": "AWS_IAM"
        }
      }
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::444455556666:role/example"
      },
      "Action": "lambda:InvokeFunction",
      "Resource": "arn:aws:lambda:us-east-1:123456789012:function:my-function",
      "Condition": {
        "Bool": {
          "lambda:InvokedViaFunctionUrl": "true"
        }
      }
    }
  ]
}
```

Vous pouvez créer cette politique basée sur les ressources via la console en suivant les étapes suivantes :

Comment accorder des autorisations d'invocation d'URL à un autre compte (console)

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez le nom de la fonction pour laquelle vous souhaitez accorder des autorisations d'invocation d'URL.
3. Choisissez l'onglet Configuration, puis Permissions (Autorisations).
4. Dans Resource-based la section Politique, choisissez Ajouter des autorisations.
5. Choisissez Function URL (URL de fonction).
6. Pour Auth type (type d'authentification), choisissez AWS_IAM (IAM_AWS).
7. Entrez un ID de déclaration pour votre déclaration de politique.

8. Pour Principal, saisissez l'ID de compte ou l'Amazon Resource Name (ARN) de l'utilisateur ou du rôle auquel vous souhaitez accorder des autorisations. Par exemple : **444455556666**.
9. Cliquez sur Enregistrer.

Vous pouvez également créer cette politique à l'aide des commandes add permission AWS Command Line Interface (AWS CLI) suivantes. Lorsque vous utilisez le AWS CLI, vous devez ajouter les `lambda:InvokeFunction` instructions `lambda:InvokeFunctionUrl` et séparément. Par exemple :

```
aws lambda add-permission --function-name my-function \
  --statement-id UrlPolicyInvokeURL \
  --action lambda:InvokeFunctionUrl \
  --principal 444455556666 \
  --function-url-auth-type AWS_IAM
```

```
aws lambda add-permission --function-name my-function \
  --statement-id UrlPolicyInvokeFunction \
  --action lambda:InvokeFunction \
  --principal 444455556666 \
  --invoked-via-function-url
```

Utilisation du type d'authentification **NONE**

> **Important**
>
> Lorsque le type d'authentification de votre URL de fonction est NONE et que vous disposez d'une politique basée sur les ressources qui accorde un accès public, tout utilisateur non authentifié ayant de votre URL de fonction peut invoquer votre fonction.

Dans certains cas, vous pouvez souhaiter que votre URL de fonction soit publique. Vus pourriez souhaiter répondre aux demandes envoyées directement à partir d'un navigateur Web. Pour autoriser l'accès public à votre URL de fonction, choisissez le type d'authentification NONE.

Si vous choisissez le NONE type d'authentification, Lambda n'utilise pas IAM pour authentifier les demandes vers votre URL de fonction. Toutefois, votre fonction doit disposer d'une politique basée sur les ressources qui autorise `lambda:InvokeFunctionUrl` et `lambda:InvokeFunction`. Lorsque vous créez une URL de fonction avec un type d'authentification à NONE l'aide de la console

ou AWS Serverless Application Model (AWS SAM), Lambda crée automatiquement la politique basée sur les ressources pour vous. Si vous utilisez directement l'API AWS CLI AWS CloudFormation, ou l'API Lambda, vous devez ajouter la politique vous-même.

Nous vous recommandons d'inclure la clé de InvokedViaFunctionUrl contexte lambda : dans vos politiques basées sur les ressources lorsque vous utilisez le `NONE` type d'authentification. Cette clé de contexte garantit que la fonction ne peut être invoquée que via l'URL de la fonction et non via d'autres méthodes d'invocation.

Notez ce qui suit concernant cette politique :

- Toutes les entités peuvent appeler `lambda:InvokeFunctionUrl` et `lambda:InvokeFunction`. Cela signifie que toute personne disposant de votre URL de fonction peut invoquer votre fonction.
- La valeur de la clé de condition `lambda:FunctionUrlAuthType` est `NONE`. Cela signifie que la déclaration de stratégie n'autorise l'accès que lorsque le type d'authentification de votre URL de fonction est également `NONE`.
- La condition `lambda:InvokedViaFunctionUrl` garantit que la fonction ne peut être invoquée que via l'URL de la fonction et non via d'autres méthodes d'invocation.

Example– Politique basée sur les ressources par défaut pour le type d'authentification NONE

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "FunctionURLAllowPublicAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "lambda:InvokeFunctionUrl",
      "Resource": "arn:aws:lambda:us-east-2:123456789012:function:my-function",
      "Condition": {
        "StringEquals": {
          "lambda:FunctionUrlAuthType": "NONE"
        }
      }
    },
```

```
    {
      "Sid": "FunctionURLInvokeAllowPublicAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "lambda:InvokeFunction",
      "Resource": "arn:aws:lambda:us-east-2:123456789012:function:my-function",
      "Condition": {
        "Bool": {
          "lambda:InvokedViaFunctionUrl": "true"
        }
      }
    }
  ]
}
```

Créez la politique basée sur les ressources à l'aide du AWS CLI

À moins que vous n'utilisiez la console ou AWS SAM que vous ne créiez une URL de fonction avec un type d'authentification`NONE`, vous devez ajouter vous-même la politique basée sur les ressources. Utilisez les commandes suivantes pour créer des instructions pour les autorisations `lambda:InvokeFunctionUrl` et `lambda:InvokeFunction`. Chaque instruction doit être ajoutée dans une commande distincte.

```
aws lambda add-permission \
  --function-name UrlTestFunction \
  --statement-id UrlPolicyInvokeURL \
  --action lambda:InvokeFunctionUrl \
  --principal * \
  --function-url-auth-type NONE
```

```
aws lambda add-permission \
  --function-name UrlTestFunction \
  --statement-id UrlPolicyInvokeFunction \
  --action lambda:InvokeFunction \
  --principal * \
  --invoked-via-function-url
```

> **Note**
>
> Si vous supprimez une URL de fonction avec un type d'authentification `NONE`, Lambda ne supprime pas automatiquement la politique basée sur les ressources associée. Si vous souhaitez supprimer cette politique, vous devez le faire manuellement.

Si la politique basée sur les ressources d'une fonction n'accorde aucune `lambda:InvokeFunction` autorisation, `lambda:invokeFunctionUrl` les utilisateurs reçoivent un code d'erreur 403 Forbidden lorsqu'ils essaient d'invoquer l'URL de votre fonction. Cela se produit même si l'URL de la fonction utilise le type d'`NONE`authentification.

Gouvernance et contrôle d'accès

Outre les autorisations d'invocation d'URL de fonction, vous pouvez également contrôler l'accès aux actions utilisées pour configurer les URL de fonctions. Lambda prend en charge les actions de stratégie IAM suivantes pour les URL de fonctions :

- `lambda:InvokeFunctionUrl`— Invoque une fonction d'événement Lambda à l'aide de l'URL de la fonction.
- `lambda:CreateFunctionUrlConfig` – Créer une URL de fonction et définir son `AuthType`.
- `lambda:UpdateFunctionUrlConfig` – Mettre à jour la configuration d'une URL de fonction et son `AuthType`.
- `lambda:GetFunctionUrlConfig` – Affichez les détails d'une URL de fonction.
- `lambda:ListFunctionUrlConfigs` – Répertorier les configurations d'URL de fonction.
- `lambda:DeleteFunctionUrlConfig` – Supprimer une URL de fonction.

Pour autoriser ou refuser l'accès à l'URL des fonctions à d'autres AWS entités, incluez ces actions dans les politiques IAM. Par exemple, la politique suivante accorde au `example` rôle dans les Compte AWS `444455556666` autorisations de mettre à jour l'URL de la fonction pour la fonction **`my-function`** dans le compte`123456789012`.

Example exemple de stratégie d'URL de fonction inter-comptes

JSON

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::444455556666:role/example"
            },
            "Action": "lambda:UpdateFunctionUrlConfig",
            "Resource": "arn:aws:lambda:us-east-2:123456789012:function:my-
function"
        }
    ]
}
```

Clés de condition

Pour un contrôle d'accès précis sur vos URL de fonctions, utilisez des clés de contexte. Lambda prend en charge les clés de contexte suivantes pour les URL de fonction :

- `lambda:FunctionUrlAuthType` : définit une valeur d'énumération décrivant le type d'authentification utilisé par l'URL de votre fonction. La valeur peut être `AWS_IAM` ou `NONE`.
- `lambda:InvokedViaFunctionUrl` : limite l'action `lambda:InvokeFunction` aux appels effectués via l'URL de la fonction. Cela garantit que la fonction ne peut être invoquée que via l'URL de la fonction et non via d'autres méthodes d'invocation. Pour des exemples de politiques basées sur les ressources qui utilisent la clé de contexte `lambda:InvokedViaFunctionUrl`, consultez les exemples dans Utilisation du type d'authentification `AWS_IAM` et Utilisation du type d'authentification `NONE`.

Vous pouvez utiliser ces clés contextuelles dans les politiques associées à votre fonction d'événement. Vous pourriez vouloir limiter les personnes pouvant apporter des modifications de configuration à vos URL de fonctions. Pour rejeter toutes les demandes `UpdateFunctionUrlConfig` à n'importe quelle fonction avec un type d'authentification URL `NONE`, vous pouvez définir la stratégie suivante :

Example exemple de stratégie d'URL de fonction avec refus explicite

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Principal": "*",
            "Action":[
                "lambda:UpdateFunctionUrlConfig"
            ],
            "Resource": "arn:aws:lambda:us-east-1:123456789012:function:*",
            "Condition": {
                "StringEquals": {
                    "lambda:FunctionUrlAuthType": "NONE"
                }
            }
        }
    ]
}
```

Pour attribuer le `example` rôle dans Compte AWS `444455556666` les autorisations de création `CreateFunctionUrlConfig` et de `UpdateFunctionUrlConfig` requêtes sur les fonctions avec un type d'authentification URL`AWS_IAM`, vous pouvez définir la politique suivante :

Example exemple de stratégie d'URL de fonction avec autorisation explicite

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::444455556666:role/example"
            },
            "Action":[
```

```
                "lambda:CreateFunctionUrlConfig",
                "lambda:UpdateFunctionUrlConfig"
            ],
            "Resource": "arn:aws:lambda:us-east-1:123456789012:function:*",
            "Condition": {
                "StringEquals": {
                    "lambda:FunctionUrlAuthType": "AWS_IAM"
                }
            }
        }
    ]
}
```

Vous pouvez également utiliser cette clé de condition dans une stratégie de contrôle de service (SCP). Utilisez les SCP pour gérer les autorisations dans toute une organisation dans AWS Organizations. Pour empêcher les utilisateurs de créer ou de mettre à jour des URL de fonctions qui utilisent autre chose que le type d'authentification `AWS_IAM`, utilisez la stratégie de contrôle de service suivante :

Example exemple d'URL de fonction SCP avec refus explicite

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action":[
                "lambda:CreateFunctionUrlConfig",
                "lambda:UpdateFunctionUrlConfig"
            ],
            "Resource": "arn:aws:lambda:*:123456789012:function:*",
            "Condition": {
                "StringNotEquals": {
                    "lambda:FunctionUrlAuthType": "AWS_IAM"
                }
            }
        }
    ]
```

```
}
```

Invocation d'URL de fonctions Lambda

L'URL d'une fonction est un point de terminaison HTTP (S) dédié à votre fonction d'événement Lambda. Vous pouvez créer et configurer une URL de fonction via la console Lambda ou l'API Lambda.

> **Tip**
>
> Lambda propose deux méthodes pour invoquer votre fonction via un point de terminaison HTTP : les URL de fonction et Amazon API Gateway. Si vous ne savez pas quelle est la meilleure méthode pour votre cas d'utilisation, consultez the section called "URL de fonction et Amazon API Gateway".

Lorsque vous créez une URL de fonction, Lambda génère automatiquement un point de terminaison URL unique pour vous. Une fois que vous avez créé une URL de fonction, son point de terminaison URL ne change jamais. Les points de terminaison URL de fonction ont le format suivant :

```
https://<url-id>.lambda-url.<region>.on.aws
```

> **Note**
>
> Les URL des fonctions ne sont pas prises en charge dans toutes les AWS régions. Pour vérifier la disponibilité, consultez la section Services AWS régionaux et filtrez par`Feature Name = Function URLs`.

Les URL de fonctions sont compatibles avec la pile double, prenant en charge les adresses IPv4 et IPv6. Après avoir configuré l'URL de votre fonction, vous pouvez appeler votre fonction via son point de terminaison HTTP (S) à l'aide d'un navigateur Web, d'un curl, de Postman ou de tout autre client HTTP. Pour invoquer l'URL d'une fonction, vous devez avoir les autorisations `lambda:InvokeFunctionUrl` et `lambda:InvokeFunction`. Pour plus d'informations, consultez Contrôle d'accès.

Rubriques

- Principes de base de l'invocation d'une URL de fonction
- Charges utiles de demandes et de réponses

Principes de base de l'invocation d'une URL de fonction

Si votre URL de votre fonction utilise le type d'authentification `AWS_IAM`, vous devez signer chaque demande HTTP en utilisant AWS Signature Version 4 (SigV4). Des outils comme Postman offrent des moyens intégrés de signer vos demandes avec SigV4.

Si vous n'utilisez pas d'outil pour signer des demandes HTTP sur l'URL de votre fonction, vous devez signer manuellement chaque demande à l'aide de SigV4. Lorsque l'URL de votre fonction reçoit une demande, Lambda calcule également la signature SigV4. Lambda traite la demande uniquement si les signatures correspondent. Pour obtenir des instructions sur la façon de signer manuellement vos demandes avec SigV4, voir Signature des AWS demandes avec signature version 4 du Référence générale d'Amazon Web Services guide.

Si l'URL de votre fonction utilise le type d'authentification `NONE`, vous n'avez pas besoin de signer vos demandes avec SigV4. Vous pouvez invoquer votre fonction via un navigateur Web, curl, Postman ou n'importe quel client HTTP.

Pour tester des demandes `GET` simples vers votre fonction, utilisez un navigateur web. Par exemple, si l'URL de votre fonction est `https://abcdefg.lambda-url.us-east-1.on.aws`, et si elle prend en compte un paramètre de chaîne `message`, l'URL de votre demande peut se présenter comme suit :

```
https://abcdefg.lambda-url.us-east-1.on.aws/?message=HelloWorld
```

Pour tester d'autres demandes HTTP, telles qu'une demande `POST`, vous pouvez utiliser un outil tel que curl. Par exemple, si vous souhaitez inclure certaines données JSON dans une demande `POST` pour l'URL de votre fonction, vous pouvez utiliser la commande curl suivante :

```
curl -v 'https://abcdefg.lambda-url.us-east-1.on.aws/?message=HelloWorld' \
-H 'content-type: application/json' \
-d '{ "example": "test" }'
```

Charges utiles de demandes et de réponses

Lorsqu'un client appelle l'URL de votre fonction, Lambda mappe la demande sur un objet événement avant de la transmettre à votre fonction. La réponse de votre fonction est ensuite mappée à une réponse HTTP que Lambda renvoie au client via l'URL de la fonction.

Les formats d'événements de demande et de réponse suivent le même schéma que le format de charge utile version 2.0 d'Amazon API Gateway.

Format de la charge utile de demande

Une charge utile de demande a la structure suivante :

```
{
  "version": "2.0",
  "routeKey": "$default",
  "rawPath": "/my/path",
  "rawQueryString": "parameter1=value1&parameter1=value2&parameter2=value",
  "cookies": [
    "cookie1",
    "cookie2"
  ],
  "headers": {
    "header1": "value1",
    "header2": "value1,value2"
  },
  "queryStringParameters": {
    "parameter1": "value1,value2",
    "parameter2": "value"
  },
  "requestContext": {
    "accountId": "123456789012",
    "apiId": "<urlid>",
    "authentication": null,
    "authorizer": {
        "iam": {
                "accessKey": "AKIA...",
                "accountId": "111122223333",
                "callerId": "AIDA...",
                "cognitoIdentity": null,
                "principalOrgId": null,
                "userArn": "arn:aws:iam::111122223333:user/example-user",
                "userId": "AIDA..."
        }
    },
    "domainName": "<url-id>.lambda-url.us-west-2.on.aws",
    "domainPrefix": "<url-id>",
    "http": {
      "method": "POST",
      "path": "/my/path",
      "protocol": "HTTP/1.1",
      "sourceIp": "123.123.123.123",
      "userAgent": "agent"
```

```
    },
    "requestId": "id",
    "routeKey": "$default",
    "stage": "$default",
    "time": "12/Mar/2020:19:03:58 +0000",
    "timeEpoch": 1583348638390
  },
  "body": "Hello from client!",
  "pathParameters": null,
  "isBase64Encoded": false,
  "stageVariables": null
}
```

Paramètre	Description	Exemple
`version`	La version du format de la charge utile pour cet événement. Les URL de fonctions Lambda prennent actuellement en charge le format de charge utile version 2.0.	`2.0`
`routeKey`	Les URL de fonctions n'utilisent pas ce paramètre. Lambda le définit sur `$default` comme espace réservé.	`$default`
`rawPath`	Chemin d'accès de la demande. Par exemple, si l'URL de la demande est `https://{url-id}.lambda-url.{region}.on.aws/example/test/demo`, alors la valeur du chemin brut est `/example/test/demo`.	`/example/test/demo`

Paramètre	Description	Exemple
`rawQueryString`	La chaîne brute contenant les paramètres de la chaîne de la requête de la demande. Les caractères pris en charge sont les suivants : `a-z`, `A-Z`, `0-9`, `.`, `_`, `-`, `%`, &, =, et +.	`"?parameter1=value1&parameter2=value2"`
`cookies`	Un tableau contenant tous les cookies envoyés dans le cadre de la demande.	`["Cookie_1=Value_1", "Cookie_2=Value_2"]`
`headers`	La liste des en-têtes de demande, présentée sous forme de paires valeur-clé.	`{"header1": "value1", "header2": "value2"}`
`queryStringParameters`	Paramètres de requête pour la demande. Par exemple, si l'URL de la demande est `https://{url-id}.lambda-url.{region}.on.aws/example?name=Jane` , alors la valeur `queryStringParameters` est un objet JSON avec une clé `name` et une valeur `Jane`.	`{"name": "Jane"}`
`requestContext`	Un objet qui contient des informations supplémentaires sur la demande, comme `requestId` , l'heure de la demande, et l'identité de l'appelant s'il est autorisé via Gestion des identités et des accès AWS (IAM).	

Paramètre	Description	Exemple
`requestContext.accountId`	Compte AWS ID du propriétaire de la fonction.	`"123456789012"`
`requestContext.apiId`	L'identifiant de l'URL de la fonction.	`"33anwqw8fj"`
`requestContext.authentication`	Les URL de fonctions n'utilisent pas ce paramètre. Lambda le définit sur `null`.	`null`
`requestContext.authorizer`	Un objet qui contient des informations sur l'identité de l'appelant si l'URL de la fonction utilise le type d'authentification `AWS_IAM`. Sinon, Lambda définit cette valeur sur `null`.	
`requestContext.authorizer.iam.accessKey`	La clé d'accès de l'identité de l'appelant.	`"AKIAIOSFODNN7EXAMPLE"`
`requestContext.authorizer.iam.accountId`	Compte AWS Identifiant de l'identité de l'appelant.	`"111122223333"`
`requestContext.authorizer.iam.callerId`	L'ID (ID d'utilisateur) de l'appelant.	`"AIDACKCEVSQ6C2EXAMPLE"`
`requestContext.authorizer.iam.cognitoIdentity`	Les URL de fonctions n'utilisent pas ce paramètre. Lambda le définit sur `null` ou l'exclut de JSON.	`null`

Paramètre	Description	Exemple
`requestContext.authorizer.iam.principalOrgId`	L'ID de l'organisation du principal associé à l'ID de l'appelant.	`"AIDACKCEVSQORGEXAMPLE"`
`requestContext.authorizer.iam.userArn`	L'Amazon Resource Name (ARN) utilisateur de l'identité de l'appelant.	`"arn:aws:iam::111122223333:user/example-user"`
`requestContext.authorizer.iam.userId`	L'identifiant utilisateur de l'identité de l'appelant.	`"AIDACOSFODNN7EXAMPLE2"`
`requestContext.domainName`	Le nom de domaine de l'URL de la fonction.	`"<url-id>.lambda-url.us-west-2.on.aws"`
`requestContext.domainPrefix`	Le nom de domaine de l'URL de la fonction.	`"<url-id>"`
`requestContext.http`	Un objet qui contient des informations sur la demande HTTP.	
`requestContext.http.method`	La méthode HTTP utilisée dans cette demande. Les valeurs valides sont les suivantes : `GET`, `POST`, `PUT`, `HEAD`, `OPTIONS`, `PATCH` et `DELETE`.	`GET`

Paramètre	Description	Exemple
`requestContext.http.path`	Chemin d'accès de la demande. Par exemple, si l'URL de la demande est `https://{url-id}.lambda-url.{region}.on.aws/example/test/demo` , alors la valeur du chemin est `/example/test/demo` .	`/example/test/demo`
`requestContext.http.protocol`	Le protocole de la demande.	`HTTP/1.1`
`requestContext.http.sourceIp`	L'adresse IP source de la connexion TCP immédiate qui fait la demande.	`123.123.123.123`
`requestContext.http.userAgent`	La valeur de l'en-tête de la User-Agent demande.	`Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) Gecko/20100101 Firefox/42.0`
`requestContext.requestId`	L'identifiant de la demande d'invocation. Vous pouvez utiliser cet ID pour suivre les journaux d'invocation liés à votre fonction.	`e1506fd5-9e7b-434f-bd42-4f8fa224b599`
`requestContext.routeKey`	Les URL de fonctions n'utilisent pas ce paramètre. Lambda le définit sur `$default` comme espace réservé.	`$default`

Paramètre	Description	Exemple
`requestContext.stage`	Les URL de fonctions n'utilisent pas ce paramètre. Lambda le définit sur `$default` comme espace réservé.	`$default`
`requestContext.time`	Horodatage de la demande.	`"07/Sep/2021:22:50:22 +0000"`
`requestContext.timeEpoch`	L'horodatage de la demande, en heure d'époque Unix.	`"1631055022677"`
`body`	Le corps de la demande. Si le type de contenu de la demande est binaire, le corps est codé en base64.	`{"key1": "value1", "key2": "value2"}`
`pathParameters`	Les URL de fonctions n'utilisent pas ce paramètre. Lambda le définit sur `null` ou l'exclut de JSON.	`null`
`isBase64Encoded`	`TRUE` si le corps est une charge utile binaire et codé en base64. Sinon `FALSE`.	`FALSE`
`stageVariables`	Les URL de fonctions n'utilisent pas ce paramètre. Lambda le définit sur `null` ou l'exclut du JSON.	`null`

Format de la charge utile de la réponse

Lorsque votre fonction renvoie une réponse, Lambda analyse la réponse et la convertit en réponse HTTP. Les charges utiles de la réponse de fonction ont le format suivant :

```
{
```

```
   "statusCode": 201,
    "headers": {
        "Content-Type": "application/json",
        "My-Custom-Header": "Custom Value"
    },
    "body": "{ \"message\": \"Hello, world!\" }",
    "cookies": [
        "Cookie_1=Value1; Expires=21 Oct 2021 07:48 GMT",
        "Cookie_2=Value2; Max-Age=78000"
    ],
    "isBase64Encoded": false
}
```

Lambda déduit le format de réponse pour vous. Si votre fonction renvoie un JSON valide et ne renvoie pas un `statusCode`, Lambda assume ce qui suit :

- `statusCode` est `200`.

> **Note**
>
> Les valeurs de `statusCode` valides sont comprises entre 100 et 599.

- `content-type` est `application/json`.
- `body` est la réponse de la fonction.
- `isBase64Encoded` est `false`.

Les exemples suivants montrent comment la sortie de votre fonction d'événement Lambda correspond à la charge utile de réponse, et comment la charge utile de réponse correspond à la réponse HTTP finale. Lorsque le client invoque l'URL de votre fonction, il voit la réponse HTTP.

Exemple de sortie pour une réponse de chaîne

Sortie de la fonction d'événement Lambda	Sortie de réponse interprétée	Réponse HTTP (ce que voit le client)
`"Hello, world!"`	`{ "statusCode": 200, "body": "Hello, world!",`	`HTTP/2 200 date: Wed, 08 Sep 2021 18:02:24 GMT`

Sortie de la fonction d'événement Lambda	Sortie de réponse interprétée	Réponse HTTP (ce que voit le client)

	<pre>"headers": {
	"content-type":
	"application/json"
	},
	"isBase64Encoded":
	false
	}</pre>
		<pre>content-type: applicati
		on/json
		content-length: 15
		
		"Hello, world!"</pre>

Exemple de sortie pour une réponse JSON

Sortie de la fonction d'événement Lambda	Sortie de réponse interprétée	Réponse HTTP (ce que voit le client)

<pre>{
"message": "Hello,
world!"
}</pre>
	<pre>{
	"statusCode": 200,
	"body": {
	"message": "Hello,
	world!"
	},
	"headers": {
	"content-type":
	"application/json"
	},
	"isBase64Encoded":
	false
	}</pre>
		<pre>HTTP/2 200
		date: Wed, 08 Sep 2021
		18:02:24 GMT
		content-type: applicati
		on/json
		content-length: 34
		
		{
		"message": "Hello,
		world!"
		}</pre>

Exemple de sortie pour une réponse personnalisée

Sortie de la fonction d'événement Lambda	Sortie de réponse interprétée	Réponse HTTP (ce que voit le client)

<pre>{
"statusCode": 201,
"headers": {</pre>
	<pre>{
	"statusCode": 201,
	"headers": {</pre>
		<pre>HTTP/2 201
		date: Wed, 08 Sep 2021
		18:02:24 GMT</pre>

Sortie de la fonction d'événement Lambda	Sortie de réponse interprétée	Réponse HTTP (ce que voit le client)

<pre>"Content-Type": "application/json", "My-Custom-Header": "Custom Value" }, "body": JSON.stringify({ "message": "Hello, world!" }), "isBase64Encoded": false }</pre>	<pre>"Content-Type": "application/json", "My-Custom-Header": "Custom Value" }, "body": JSON.stringify({ "message": "Hello, world!" }), "isBase64Encoded": false }</pre>	<pre>content-type: application/json content-length: 27 my-custom-header: Custom Value
		
		{ "message": "Hello, world!" }</pre>

Cookies

Pour renvoyer des cookies depuis votre fonction, n'ajoutez pas manuellement des en-têtes `set-cookie`. Incluez plutôt les cookies dans votre objet de charge utile de réponse. Lambda les interprète automatiquement et les ajoute comme en-têtes `set-cookie` de votre réponse HTTP, comme dans l'exemple suivant.

Sortie de la fonction d'événement Lambda	Réponse HTTP (ce que voit le client)

<pre>{ "statusCode": 201, "headers": { "Content-Type": "application/json", "My-Custom-Header": "Custom Value" }, "body": JSON.stringify({ "message": "Hello, world!" }), "cookies": ["Cookie_1=Value1; Expires=21 Oct 2021 07:48 GMT",</pre>	<pre>HTTP/2 201 date: Wed, 08 Sep 2021 18:02:24 GMT content-type: application/json content-length: 27 my-custom-header: Custom Value set-cookie: Cookie_1=Value2; Expires=21 Oct 2021 07:48 GMT set-cookie: Cookie_2=Value2; Max-Age=78000
	
	{ "message": "Hello, world!" }</pre>

Sortie de la fonction d'événement Lambda	Réponse HTTP (ce que voit le client)

```
        "Cookie_2=Value2; Max-Age=7
8000"
    ],
    "isBase64Encoded": false
}
```

Surveillance des URL de fonctions Lambda

Vous pouvez utiliser AWS CloudTrail et Amazon CloudWatch pour surveiller vos URL de fonctions.

Rubriques

- URL de fonctions de surveillance avec CloudTrail
- Métriques CloudWatch pour les URL de fonctions

URL de fonctions de surveillance avec CloudTrail

Pour les URL de fonctions, Lambda prend automatiquement en charge la journalisation des opérations API suivantes en tant qu'événements dans des fichiers journaux CloudTrail :

- CreateFunctionUrlConfig
- UpdateFunctionUrlConfig
- DeleteFunctionUrlConfig
- GetFunctionUrlConfig
- ListFunctionUrlConfigs

Chaque entrée de journal contient des informations sur l'identité de l'appelant, le moment où la demande a été faite, et d'autres détails. Vous pouvez voir tous les événements des 90 derniers jours en consultant votre Event history (Historique des événements) CloudTrail. Pour conserver les enregistrements de plus de 90 jours, vous pouvez créer un journal d'activité.

Par défaut, CloudTrail ne journalise pas les demandes `InvokeFunctionUrl`, qui sont considérées comme des événements de données. Cependant, vous pouvez activer la journalisation des événements de données dans CloudTrail. Pour plus d'informations, consultez Consignation d'événements de données pour les journaux d'activité dans le Guide de l'utilisateur AWS CloudTrail.

Métriques CloudWatch pour les URL de fonctions

Lambda envoie des métriques agrégées concernant les demandes d'URL de fonction vers CloudWatch. Avec ces métriques, vous pouvez surveiller les URL de vos fonctions, créer des tableaux de bord et configurer des alarmes dans la console CloudWatch.

Les URL de fonctions prennent en charge les métriques d'invocation suivantes. Nous vous recommandons de consulter ces métriques avec la statistique `Sum`.

- `UrlRequestCount` – Nombre de demandes faites vers cette URL de fonction.
- `Url4xxCount` – Nombre de demandes ayant retourné un code d'état HTTP 4XX. Les codes de la série 4XX indiquent des erreurs côté client, telles que des demandes erronées.
- `Url5xxCount` – Nombre de demandes ayant retourné un code d'état HTTP 5XX. Les codes de la série 5XX indiquent des erreurs côté serveur, telles que des erreurs de fonction et des délais d'attente.

Les URL de fonctions prennent également en charge la métrique de performance suivante. Nous vous recommandons de consulter ces métriques avec les statistiques `Average` ou `Max`.

- `UrlRequestLatency` – Le temps écoulé entre le moment où l'URL de fonction reçoit une demande et celui où l'URL de fonction renvoie une réponse.

Chacune de ces métriques d'invocation et de performance prend en charge les dimensions suivantes :

- `FunctionName` – Affichez les métriques agrégées pour les URL de fonctions attribuées à la version non publiée `$LATEST` d'une fonction, ou à tout alias de la fonction. Par exemple, `hello-world-function`.
- `Resource` – Affichez les métriques d'une URL de fonction spécifique. Cela est défini par un nom de fonction, accompagné de la version non publiée `$LATEST` de la fonction ou d'un alias de la fonction. Par exemple, `hello-world-function:$LATEST`.
- `ExecutedVersion` – Affichez les métriques d'une URL de fonction spécifique en fonction de la version exécutée. Vous pouvez utiliser cette dimension principalement pour suivre l'URL de la fonction affectée à la version non publiée `$LATEST`.

Sélectionnez une méthode pour appeler votre fonction d'événement Lambda à l'aide d'une requête HTTP

De nombreux cas d'utilisation courants de Lambda impliquent l'appel de votre fonction d'événement à l'aide d'une requête HTTP. Vous pourriez souhaiter qu’une application Web invoque votre fonction par le biais d’une demande de navigateur. Les fonctions d'événement Lambda peuvent également être utilisées pour créer des API REST complètes, gérer les interactions des utilisateurs à partir d'applications mobiles, traiter des données provenant de services externes via des appels HTTP ou créer des webhooks personnalisés.

Les sections suivantes expliquent quels sont vos choix pour invoquer Lambda via HTTP et fournissent des informations qui vous aideront à prendre la bonne décision pour votre cas d'utilisation particulier.

Options proposées lors de la sélection d'une méthode d'appel HTTP

Lambda propose deux méthodes principales pour invoquer une fonction à l'aide d'une requête HTTP : les URL de fonctions et API Gateway. Les principales différences entre ces deux options sont les suivantes :

- Les URL des fonctions Lambda fournissent un point de terminaison HTTP simple et direct pour une fonction d'événement Lambda. Ils sont optimisés pour des raisons de simplicité et de rentabilité et constituent le moyen le plus rapide d'exposer une fonction d'événement Lambda via HTTP.
- API Gateway est un service plus avancé permettant de créer des API complètes. API Gateway est optimisé pour créer et gérer des API de production à grande échelle et fournit des outils complets pour la sécurité, la surveillance et la gestion du trafic.

Recommandations si vous connaissez déjà vos besoins

Si vous connaissez déjà bien vos besoins, voici nos recommandations de base :

Nous recommandons les URL de fonction pour les applications simples ou le prototypage lorsque vous n'avez besoin que de méthodes d'authentification et de request/response manipulation de base et lorsque vous souhaitez réduire les coûts et la complexité au minimum.

API Gateway est un meilleur choix pour les applications de production à grande échelle ou pour les cas où vous avez besoin de fonctionnalités plus avancées telles que la prise en charge d'OpenAPI Description, un choix d'options d'authentification, des noms de domaine personnalisés ou une request/response gestion riche, notamment la régulation, la mise en cache et la transformation. request/response

Éléments à prendre en compte lors de la sélection d'une méthode pour appeler votre fonction d'événement Lambda

Lorsque vous choisissez entre les URL de fonctions et API Gateway, vous devez prendre en compte les facteurs suivants :

- Vos besoins en matière d'authentification, par exemple si vous avez besoin d'OAuth ou d'Amazon Cognito pour authentifier les utilisateurs

- Vos exigences en matière de mise à l'échelle et la complexité de l'API que vous souhaitez implémenter
- Si vous avez besoin de fonctionnalités avancées telles que la validation et le request/response formatage des demandes
- Vos besoins en matière de surveillance
- Vos objectifs en matière de coûts

La compréhension de ces facteurs vous permettra de choisir l'option qui répond le mieux à vos exigences en matière de sécurité, de complexité et de coût.

Le tableau suivant résume les différences entre les deux options.

Authentification

- Les URL des fonctions fournissent des options d'authentification de base via Gestion des identités et des accès AWS (IAM). Vous pouvez configurer vos points de terminaison pour qu'ils soient publics (aucune authentification) ou pour qu'ils nécessitent une authentification IAM. Avec l'authentification IAM, vous pouvez utiliser des AWS informations d'identification standard ou des rôles IAM pour contrôler l'accès. Bien que simple à configurer, cette approche offre des options limitées par rapport aux autres méthodes d'authentification.
- API Gateway donne accès à une gamme plus complète d'options d'authentification. Outre l'authentification IAM, vous pouvez utiliser les autorisateurs Lambda (logique d'authentification personnalisée), les groupes d'utilisateurs et les flux Amazon Cognito. OAuth2.0 Cette flexibilité vous permet de mettre en œuvre des schémas d'authentification complexes, notamment des fournisseurs d'authentification tiers, une authentification basée sur des jetons et une authentification multifactorielle.

Request/response manipulation

- Les URL de fonctions fournissent une gestion de base des requêtes et des réponses HTTP. Elles prennent en charge les méthodes HTTP standard et créent une prise en charge intégrée du partage des ressources entre origines (CORS, cross-origin resource sharing). Bien qu'elles puissent gérer naturellement les charges utiles JSON et les paramètres de requête, elles n'offrent pas de fonctionnalités de transformation ou de validation des requêtes. La gestion des réponses est tout aussi simple : le client reçoit la réponse de votre fonction d'événement Lambda exactement telle que Lambda la renvoie.

- API Gateway fournit des fonctionnalités sophistiquées de gestion des requêtes et des réponses. Vous pouvez définir des validateurs de demandes, transformer les demandes et les réponses à l'aide de modèles de mappage, configurer request/response des en-têtes et implémenter la mise en cache des réponses. API Gateway prend également en charge les charges utiles binaires et les noms de domaine personnalisés et peut modifier les réponses avant qu'elles n'atteignent le client. Vous pouvez configurer des modèles pour la request/response validation et la transformation à l'aide du schéma JSON.

Mise à l'échelle

- Les URL des fonctions s'adaptent directement aux limites de simultanéité de votre fonction d'événement Lambda et gèrent les pics de trafic en redimensionnant votre fonction jusqu'à sa limite de simultanéité maximale configurée. Une fois cette limite atteinte, Lambda répond aux requêtes supplémentaires avec des réponses HTTP 429. Il n'existe aucun mécanisme de mise en file d'attente intégré. La gestion du dimensionnement dépend donc entièrement de la configuration de votre fonction d'événement Lambda. Par défaut, les fonctions d'événement Lambda sont limitées à 1 000 exécutions simultanées par. Région AWS
- API Gateway fournit des fonctionnalités de dimensionnement supplémentaires en plus de la propre mise à l'échelle de Lambda. Il inclut des commandes intégrées de mise en file d'attente et de limitation des requêtes, ce qui vous permet de gérer les pics de trafic de manière plus élégante. API Gateway peut traiter jusqu'à 10 000 requêtes par seconde et par région par défaut, avec une capacité de débordement de 5 000 requêtes par seconde. Il fournit également des outils pour limiter les requêtes à différents niveaux (API, étape ou méthode) afin de protéger votre dorsal.

Contrôle

- Les URL des fonctions offrent une surveillance de base via CloudWatch les métriques Amazon, notamment le nombre de demandes, la latence et les taux d'erreur. Vous avez accès aux métriques et aux journaux Lambda standard, qui indiquent les requêtes brutes entrant dans votre fonction. Bien que cela fournisse une visibilité opérationnelle essentielle, les métriques se concentrent principalement sur l'exécution des fonctions.
- API Gateway fournit des fonctionnalités de surveillance complètes, notamment des métriques détaillées, des options de journalisation et de suivi. Vous pouvez surveiller les appels d'API, la latence, les taux d'erreur et hit/miss les taux de cache via CloudWatch. API Gateway s'intègre également au AWS X-Ray traçage distribué et fournit des formats de journalisation personnalisables.

Coût

- Les URL de fonctions suivent le modèle de tarification Lambda standard : vous ne payez que pour les appels de fonctions et le temps de calcul. Il n'y a pas de frais supplémentaires pour le point de terminaison de l'URL lui-même. Cela en fait un choix rentable pour les API simples ou les applications à faible trafic si vous n'avez pas besoin des fonctionnalités supplémentaires d'API Gateway.
- API Gateway propose un niveau gratuit qui inclut un million d'appels d'API reçus pour les API REST et un million d'appels d'API reçus pour les API HTTP. Ensuite, API Gateway facture les appels d'API, le transfert de données et la mise en cache (si activée). Reportez-vous à la page de tarification d'API Gateway pour connaître les coûts associés à votre propre cas d'utilisation.

Autres fonctions

- Les URL de fonctions sont conçues dans un souci de simplicité et d'intégration directe avec Lambda. Elles prennent en charge les points de terminaison HTTP et HTTPS, offrent une prise en charge CORS intégrée et créent des points de terminaison à double pile (IPv4 et IPv6). Bien qu'ils ne disposent pas de fonctionnalités avancées, ils excellent dans les scénarios où vous avez besoin d'un moyen simple et rapide d'exposer les fonctions d'événement Lambda via HTTP.
- API Gateway inclut de nombreuses fonctionnalités supplémentaires telles que le versionnement des API, la gestion des étapes, les clés d'API pour les plans d'utilisation, la documentation des API, les WebSocket API Swagger/OpenAPI, les API privées au sein d'un VPC et l'intégration WAF pour une sécurité accrue. Il prend également en charge les déploiements Canary, les intégrations fictives à des fins de test et l'intégration avec d'autres solutions que Services AWS Lambda.

Sélectionnez une méthode pour appeler votre fonction d'événement Lambda

Maintenant que vous avez pris connaissance des critères de sélection entre les URL de fonctions Lambda et API Gateway et des principales différences entre les deux, vous pouvez sélectionner l'option qui répond le mieux à vos besoins et utiliser les ressources suivantes pour vous aider à commencer à l'utiliser.

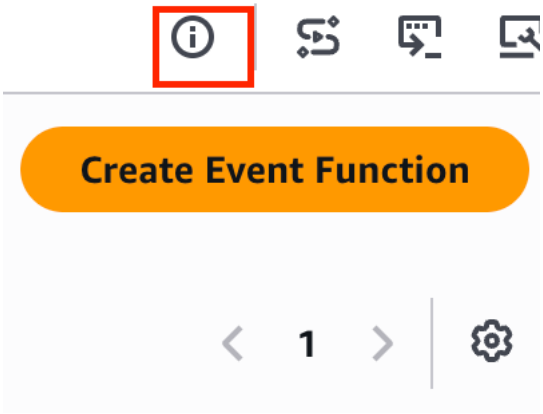
Function URLs

Mise en route avec les URL de fonctions grâce aux ressources suivantes

- Suivez le didacticiel Création d'une fonction d'événement Lambda avec une URL de fonction

- Pour en savoir plus sur les URL de fonctions, consultez le chapitre the section called “URL de fonctions” de ce guide
- Essayez le tutoriel guidé intégré à la console Créer une application Web simple en procédant comme suit :

1. Ouvrez la page Event Functions de la console Lambda.
2. Ouvrez le panneau d’aide en cliquant sur l’icône dans le coin supérieur droit de l’écran.



3. Sélectionnez Tutoriels.
4. Dans Créer une application Web simple, choisissez Démarrer le tutoriel.

API Gateway

Mise en route avec Lambda et API Gateway grâce aux ressources suivantes

- Suivez le didacticiel Utilisation de Lambda avec API Gateway pour créer une API REST intégrée à une fonction d'événement Lambda principale.
- Pour en savoir plus sur les différents types d’API proposés par API Gateway, consultez les sections suivantes du Guide du développeur Amazon API Gateway :
  - API REST d’API Gateway
  - API HTTP d’API Gateway
  - API Gateway (WebSocket API)
- Essayez un ou plusieurs des exemples de la section Tutoriels et ateliers du manuel Guide du développeur Amazon API Gateway.

Didacticiel : création d'un point de terminaison webhook à l'aide d'une URL de fonction Lambda

Dans ce didacticiel, vous créez une URL de fonction Lambda pour implémenter un point de terminaison webhook. Un webhook est une communication légère pilotée par les événements qui envoie automatiquement des données entre applications via HTTP. Vous pouvez utiliser un webhook pour recevoir des mises à jour immédiates sur les événements survenant dans un autre système, par exemple lorsqu'un nouveau client s'inscrit sur un site Web, qu'un paiement est traité ou qu'un fichier est chargé.

Avec Lambda, les webhooks peuvent être implémentés à l'aide d'URL de fonction Lambda ou d'API Gateway. Les URL de fonction sont un bon choix pour les webhooks simples qui ne nécessitent pas de fonctionnalités comme l'autorisation avancée ou la validation des demandes.

> **Tip**
>
> Si vous ne savez pas quelle est la solution la mieux adaptée à votre cas d'utilisation particulier, consultez the section called "URL de fonction et Amazon API Gateway".

Conditions préalables

Pour terminer ce didacticiel, Python (version 3.8 ou ultérieure) ou Node.js (version 18 ou ultérieure) doit être installé sur votre machine locale.

Pour tester le point de terminaison à l'aide d'une requête HTTP, le didacticiel utilise curl, un outil de ligne de commande que vous pouvez utiliser pour transférer des données à l'aide de différents protocoles réseau. Reportez-vous à la documentation curl pour savoir comment installer l'outil si vous ne l'avez pas déjà.

Création de la fonction d'événement Lambda

Créez d'abord la fonction d'événement Lambda qui s'exécute lorsqu'une requête HTTP est envoyée à votre point de terminaison Webhook. Dans cet exemple, l'application d'envoi envoie une mise à jour chaque fois qu'un paiement est soumis, et indique dans le corps de la requête HTTP si le paiement a été effectué avec succès. La fonction d'événement Lambda analyse la demande et prend des mesures en fonction du statut du paiement. Dans cet exemple, le code imprime simplement l'ID de commande pour le paiement, mais dans une application réelle, vous pouvez ajouter la commande à une base de données ou envoyer une notification.

La fonction implémente également la méthode d'authentification la plus couramment utilisée pour les webhooks, l'authentification des messages basée sur le hachage (HMAC). Avec cette méthode, les applications d'envoi et de réception partagent une clé secrète. L'application d'envoi utilise un algorithme de hachage pour générer une signature unique à l'aide de cette clé associée au contenu du message, et inclut la signature dans la demande de webhook sous forme d'en-tête HTTP. L'application réceptrice répète ensuite cette étape en générant la signature à l'aide de la clé secrète, et compare la valeur obtenue avec la signature envoyée dans l'en-tête de la demande. Si le résultat correspond, la demande est considérée comme légitime.

Créez la fonction à l'aide de la console Lambda avec Python ou Node.js un moteur d'exécution.

Python

Création de la fonction d'événement Lambda

1. Ouvrez la page Event Functions de la console Lambda.
2. Créez une fonction de type « Hello World » de base en procédant comme suit :
   a. Choisissez Create Event Function.
   b. Sélectionnez Créer à partir de zéro.
   c. Sous Nom de la fonction, saisissez **`myLambdaWebhook`**.
   d. Pour Runtime, sélectionnez python3.14.
   e. Choisissez Create Event Function.
3. Dans le volet Source du code, remplacez le code existant en copiant et en collant ce qui suit :

```
import json
import hmac
import hashlib
import os

def lambda_handler(event, context):

    # Get the webhook secret from environment variables
    webhook_secret = os.environ['WEBHOOK_SECRET']

    # Verify the webhook signature
    if not verify_signature(event, webhook_secret):
        return {
            'statusCode': 401,
            'body': json.dumps({'error': 'Invalid signature'})
```

```
        }

    try:
        # Parse the webhook payload
        payload = json.loads(event['body'])

        # Handle different event types
        event_type = payload.get('type')

        if event_type == 'payment.success':
            # Handle successful payment
            order_id = payload.get('orderId')
            print(f"Processing successful payment for order {order_id}")

            # Add your business logic here
            # For example, update database, send notifications, etc.

        elif event_type == 'payment.failed':
            # Handle failed payment
            order_id = payload.get('orderId')
            print(f"Processing failed payment for order {order_id}")

            # Add your business logic here

        else:
            print(f"Received unhandled event type: {event_type}")

        # Return success response
        return {
            'statusCode': 200,
            'body': json.dumps({'received': True})
        }

    except json.JSONDecodeError:
        return {
            'statusCode': 400,
            'body': json.dumps({'error': 'Invalid JSON payload'})
        }
    except Exception as e:
        print(f"Error processing webhook: {e}")
        return {
            'statusCode': 500,
            'body': json.dumps({'error': 'Internal server error'})
        }
```

```
def verify_signature(event, webhook_secret):
    """
    Verify the webhook signature using HMAC
    """
    try:
        # Get the signature from headers
        signature = event['headers'].get('x-webhook-signature')

        if not signature:
            print("Error: Missing webhook signature in headers")
            return False

        # Get the raw body (return an empty string if the body key doesn't
 exist)
        body = event.get('body', '')

        # Create HMAC using the secret key
        expected_signature = hmac.new(
            webhook_secret.encode('utf-8'),
            body.encode('utf-8'),
            hashlib.sha256
        ).hexdigest()

        # Compare the expected signature with the received signature to
 authenticate the message
        is_valid = hmac.compare_digest(signature, expected_signature)
        if not is_valid:
            print(f"Error: Invalid signature. Received: {signature}, Expected:
 {expected_signature}")
            return False

        return True
    except Exception as e:
        print(f"Error verifying signature: {e}")
        return False
```

4. Dans la section DÉPLOYER, choisissez Déployer pour mettre à jour le code de votre fonction.

Node.js

Création de la fonction d'événement Lambda

1. Ouvrez la page Event Functions de la console Lambda.
2. Créez une fonction de type « Hello World » de base en procédant comme suit :
   a. Choisissez Create Event Function.
   b. Sélectionnez Créer à partir de zéro.
   c. Sous Nom de la fonction, saisissez **myLambdaWebhook**.
   d. Pour Runtime, sélectionnez nodejs24.x.
   e. Choisissez Create Event Function.
3. Dans le volet Source du code, remplacez le code existant en copiant et en collant ce qui suit :

```
import crypto from 'crypto';

export const handler = async (event, context) => {
    // Get the webhook secret from environment variables
    const webhookSecret = process.env.WEBHOOK_SECRET;

    // Verify the webhook signature
    if (!verifySignature(event, webhookSecret)) {
        return {
            statusCode: 401,
            body: JSON.stringify({ error: 'Invalid signature' })
        };
    }

    try {
        // Parse the webhook payload
        const payload = JSON.parse(event.body);

        // Handle different event types
        const eventType = payload.type;

        switch (eventType) {
            case 'payment.success': {
                // Handle successful payment
                const orderId = payload.orderId;
                console.log(`Processing successful payment for order
 ${orderId}`);
```

```
                // Add your business logic here
                // For example, update database, send notifications, etc.
                break;
            }

            case 'payment.failed': {
                // Handle failed payment
                const orderId = payload.orderId;
                console.log(`Processing failed payment for order ${orderId}`);

                // Add your business logic here
                break;
            }

            default:
                console.log(`Received unhandled event type: ${eventType}`);
        }

        // Return success response
        return {
            statusCode: 200,
            body: JSON.stringify({ received: true })
        };

    } catch (error) {
        if (error instanceof SyntaxError) {
            // Handle JSON parsing errors
            return {
                statusCode: 400,
                body: JSON.stringify({ error: 'Invalid JSON payload' })
            };
        }

        // Handle all other errors
        console.error('Error processing webhook:', error);
        return {
            statusCode: 500,
            body: JSON.stringify({ error: 'Internal server error' })
        };
    }
};

// Verify the webhook signature using HMAC
```

```
const verifySignature = (event, webhookSecret) => {
    try {
        // Get the signature from headers
        const signature = event.headers['x-webhook-signature'];

        if (!signature) {
            console.log('No signature found in headers:', event.headers);
            return false;
        }

        // Get the raw body (return an empty string if the body key doesn't
 exist)
        const body = event.body || '';

        // Create HMAC using the secret key
        const hmac = crypto.createHmac('sha256', webhookSecret);
        const expectedSignature = hmac.update(body).digest('hex');

        // Compare expected and received signatures
        const isValid = signature === expectedSignature;
        if (!isValid) {
            console.log(`Invalid signature. Received: ${signature}, Expected:
 ${expectedSignature}`);
            return false;
        }

        return true;
    } catch (error) {
        console.error('Error during signature verification:', error);
        return false;
    }
 };
```

4. Dans la section DÉPLOYER, choisissez Déployer pour mettre à jour le code de votre fonction.

Créer la clé de secret

Pour que la fonction d'événement Lambda authentifie la demande de webhook, elle utilise une clé secrète qu'elle partage avec l'application appelante. Dans cet exemple, la clé est stockée dans une variable d’environnement. Dans une application de production, n’incluez pas d’informations sensibles

telles que des mots de passe dans votre code de fonction. Créez plutôt un AWS Secrets Manager secret, puis utilisez l'extension Lambda AWS Parameters and Secrets pour récupérer vos informations d'identification dans votre fonction d'événement Lambda.

Créer et stocker la clé secrète du webhook

1. Générez une longue chaîne aléatoire à l'aide d'un générateur de nombres aléatoires sécurisé par cryptographie. Vous pouvez utiliser les extraits de code suivants en Python ou Node.js pour générer et imprimer un secret de 32 caractères, ou utiliser votre propre méthode préférée.

   Python

   Example code pour générer un secret

   ```
   import secrets
   webhook_secret = secrets.token_urlsafe(32)
   print(webhook_secret)
   ```

   Node.js

   Example code pour générer un secret (format du module ES)

   ```
   import crypto from 'crypto';
   let webhookSecret = crypto.randomBytes(32).toString('base64');
   console.log(webhookSecret)
   ```

2. Stockez la chaîne générée en tant que variable d'environnement pour votre fonction en procédant comme suit :

   a. Dans l'onglet Configuration de votre fonction, sélectionnez Variables d'environnement.

   b. Choisissez Modifier.

   c. Choisissez Ajouter une variable d'environnement.

   d. Pour Clé, saisissez **`WEBHOOK_SECRET`**, puis pour Valeur, saisissez le secret que vous avez généré à l'étape précédente.

   e. Cliquez sur Enregistrer.

Vous devrez réutiliser ce secret ultérieurement dans le didacticiel pour tester votre fonction. Veillez donc à le noter dès maintenant.

Créer le point de terminaison d'URL de fonction

Créez un point de terminaison pour votre webhook à l'aide d'une URL de fonction Lambda. Comme vous utilisez le type d'authentification `NONE` pour créer un point de terminaison avec accès public, toute personne disposant de l'URL peut invoquer votre fonction. Pour en savoir plus sur le contrôle de l'accès aux URL de fonction, consultez the section called "Contrôle d'accès". Si vous avez besoin d'options d'authentification plus avancées pour votre webhook, pensez à utiliser API Gateway.

Créer le point de terminaison d'URL de fonction

1. Dans l'onglet Configuration de votre fonction événementielle, sélectionnez URL de la fonction.
2. Choisissez Create function URL (Créer une URL de fonction).
3. Pour Type d'authentification, sélectionnez NONE.
4. Cliquez sur Enregistrer.

Le point de terminaison de l'URL de fonction que vous venez de créer s'affiche dans le volet URL de fonction. Copiez le point de terminaison ; vous l'utiliserez ultérieurement dans le didacticiel.

Testez la fonction d'événement dans la console

Avant d'utiliser une requête HTTP pour appeler votre fonction d'événement à l'aide du point de terminaison de l'URL, testez-la dans la console pour vérifier que votre code fonctionne comme prévu.

Pour vérifier la fonction d'événement dans la console, vous devez d'abord calculer une signature webhook en utilisant le secret que vous avez généré plus tôt dans le didacticiel avec la charge utile JSON de test suivante :

```
{
    "type": "payment.success",
    "orderId": "1234",
    "amount": "99.99"
}
```

Utilisez l'un des exemples de Node.js code ou de Python suivants pour calculer la signature du webhook à l'aide de votre propre secret.

Python

Calculer la signature du webhook

1. Enregistrez le code suivant dans un fichier nommé `calculate_signature.py`. Remplacez le secret de webhook dans le code par votre propre valeur.

```
import secrets
import hmac
import json
import hashlib

webhook_secret = "arlbSDCP86n_1H90s0fL_Qb2NAHBIBQOyGI0X4Zay4M"

body = json.dumps({"type": "payment.success", "orderId": "1234", "amount":
 "99.99"})

signature = hmac.new(
            webhook_secret.encode('utf-8'),
            body.encode('utf-8'),
            hashlib.sha256
        ).hexdigest()

print(signature)
```

2. Calculez la signature en exécutant la commande suivante à partir du répertoire où vous avez enregistré le code. Copiez la signature émise par le code.

```
python calculate_signature.py
```

Node.js

Calculer la signature du webhook

1. Enregistrez le code suivant dans un fichier nommé `calculate_signature.mjs`. Remplacez le secret de webhook dans le code par votre propre valeur.

```
import crypto from 'crypto';

const webhookSecret = "arlbSDCP86n_1H90s0fL_Qb2NAHBIBQOyGI0X4Zay4M"
```

```
const body = "{\"type\": \"payment.success\", \"orderId\": \"1234\", \"amount\":
 \"99.99\"}";

let hmac = crypto.createHmac('sha256', webhookSecret);
let signature = hmac.update(body).digest('hex');

console.log(signature);
```

2. Calculez la signature en exécutant la commande suivante à partir du répertoire où vous avez enregistré le code. Copiez la signature émise par le code.

```
node calculate_signature.mjs
```

Vous pouvez désormais tester le code de votre fonction à l'aide d'une requête HTTP de test dans la console.

Testez la fonction d'événement dans la console

1. Sélectionnez l'onglet Code correspondant à votre fonction événementielle.
2. Dans la section ÉVÉNEMENTS DE TEST, choisissez Créer un nouvel événement de test.
3. Dans Event Name (Nom de l'événement), saisissez **myEvent**.
4. Remplacez le JSON existant en copiant et en collant ce qui suit dans le volet JSON d'événement. Remplacez la signature de webhook par la valeur calculée à l'étape précédente.

```
{
  "headers": {
    "Content-Type": "application/json",
    "x-webhook-signature":
 "2d672e7a0423fab740fbc040e801d1241f2df32d2ffd8989617a599486553e2a"
  },
  "body": "{\"type\": \"payment.success\", \"orderId\": \"1234\", \"amount\":
 \"99.99\"}"
}
```

5. Cliquez sur Enregistrer.
6. Sélectionnez Invoquer .

Vous devez voir des résultats similaires à ce qui suit :

Python

```
Status: Succeeded
Test Event Name: myEvent

Response:
{
  "statusCode": 200,
  "body": "{\"received\": true}"
}

Function Logs:
START RequestId: 50cc0788-d70e-453a-9a22-ceaa210e8ac6 Version: $LATEST
Processing successful payment for order 1234
END RequestId: 50cc0788-d70e-453a-9a22-ceaa210e8ac6
REPORT RequestId: 50cc0788-d70e-453a-9a22-ceaa210e8ac6 Duration: 1.55 ms Billed
 Duration: 2 ms Memory Size: 128 MB Max Memory Used: 36 MB Init Duration: 136.32
 ms
```

Node.js

```
Status: Succeeded
Test Event Name: myEvent

Response:
{
  "statusCode": 200,
  "body": "{\"received\":true}"
}

Function Logs:
START RequestId: e54fe6c7-1df9-4f05-a4c4-0f71cacd64f4 Version: $LATEST
2025-01-10T18:05:42.062Z e54fe6c7-1df9-4f05-a4c4-0f71cacd64f4 INFO Processing
 successful payment for order 1234
END RequestId: e54fe6c7-1df9-4f05-a4c4-0f71cacd64f4
REPORT RequestId: e54fe6c7-1df9-4f05-a4c4-0f71cacd64f4 Duration: 60.10 ms Billed
 Duration: 61 ms Memory Size: 128 MB Max Memory Used: 72 MB Init Duration:
 174.46 ms

Request ID: e54fe6c7-1df9-4f05-a4c4-0f71cacd64f4
```

Testez la fonction d'événement à l'aide d'une requête HTTP

Utilisez l’outil de ligne de commande curl pour tester votre point de terminaison webhook.

Testez la fonction d'événement à l'aide de requêtes HTTP

1. Dans un terminal ou un programme shell, exécutez la commande curl suivante. Remplacez l’URL par la valeur du point de terminaison de votre URL de fonction et remplacez la signature du webhook par la signature que vous avez calculée à l’aide de votre propre clé secrète.

```
curl -X POST https://ryqgmbx5xjzxahif6frvzikpre0bpvpf.lambda-url.us-west-2.on.aws/
 \
-H "Content-Type: application/json" \
-H "x-webhook-
signature: d5f52b76ffba65ff60ea73da67bdf1fc5825d4db56b5d3ffa0b64b7cb85ef48b" \
-d '{"type": "payment.success", "orderId": "1234", "amount": "99.99"}'
```

   Vous devriez voir la sortie suivante :

```
{"received": true}
```

2. Examinez les CloudWatch journaux de votre fonction pour confirmer qu'elle a correctement analysé la charge utile en procédant comme suit :

   a. Ouvrez la page du groupe Logs dans la CloudWatch console Amazon.

   b. Sélectionnez le groupe de journaux de votre fonction (`/aws/lambda/myLambdaWebhook`).

   c. Sélectionnez le flux de journaux le plus récent.

      Vous devez voir des résultats similaires à ce qui suit dans les journaux de votre fonction :

      Python

```
Processing successful payment for order 1234
```

      Node.js

```
2025-01-10T18:05:42.062Z e54fe6c7-1df9-4f05-a4c4-0f71cacd64f4 INFO
 Processing successful payment for order 1234
```

3. Confirmez que votre code détecte une signature non valide en exécutant la commande curl suivante. Remplacez l'URL par le point de terminaison de l'URL de votre propre fonction.

```
curl -X POST https://ryqgmbx5xjzxahif6frvzikpre0bpvpf.lambda-url.us-west-2.on.aws/
 \
-H "Content-Type: application/json" \
-H "x-webhook-signature: abcdefg" \
-d '{"type": "payment.success", "orderId": "1234", "amount": "99.99"}'
```

Vous devriez voir la sortie suivante :

```
{"error": "Invalid signature"}
```

Nettoyage de vos ressources

Vous pouvez maintenant supprimer les ressources que vous avez créées pour ce didacticiel, sauf si vous souhaitez les conserver. En supprimant AWS les ressources que vous n'utilisez plus, vous évitez des frais inutiles pour votre Compte AWS.

Pour supprimer la fonction d'événement Lambda

1. Ouvrez la page Event Functions de la console Lambda.
2. Sélectionnez la fonction d'événement que vous avez créée.
3. Sélectionnez Actions, Supprimer.
4. Saisissez **`confirm`** dans la zone de saisie de texte et choisissez Delete (Supprimer).

Lorsque vous avez créé la fonction d'événement Lambda dans la console, Lambda a également créé un rôle d'exécution pour votre fonction.

Pour supprimer le rôle d'exécution

1. Ouvrez la page Roles (Rôles) de la console IAM.
2. Sélectionnez le rôle d'exécution que Lambda a créé. Le nom du rôle est au format `myLambdaWebhook-role-<random string>`.
3. Sélectionnez Supprimer.
4. Saisissez le nom du rôle dans le champ de saisie de texte et choisissez Delete (Supprimer).

Comprendre le dimensionnement des fonctions d'événement Lambda

La simultanéité est le nombre de demandes en cours de vol traitées simultanément par votre fonction AWS Lambda événementielle. Pour chaque demande simultanée, Lambda fournit une instance distincte de votre environnement d'exécution. Au fur et à mesure que vos fonctions événementielles reçoivent de plus en plus de demandes, Lambda gère automatiquement le dimensionnement du nombre d'environnements d'exécution jusqu'à ce que vous atteigniez la limite de simultanéité de votre compte. Par défaut, Lambda fournit à votre compte une limite de simultanéité totale de 1 000 exécutions simultanées pour toutes les fonctions d'événement d'un. Région AWS Pour répondre aux besoins spécifiques de votre compte, vous pouvez demander une augmentation du quota et configurer des contrôles de simultanéité au niveau des fonctions afin que vos fonctions d'événements critiques ne soient pas limitées.

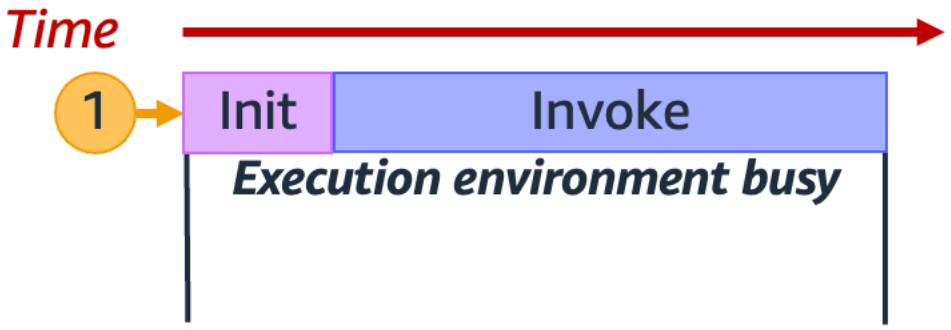
Cette rubrique explique les concepts de simultanéité et le dimensionnement des fonctions d'événement dans Lambda. À la fin de cette rubrique, vous serez en mesure de comprendre comment calculer la simultanéité, de visualiser les deux principales options de contrôle de la simultanéité (réservée et provisionnée), d'estimer les paramètres de contrôle de la simultanéité appropriés et de visualiser les métriques pour une optimisation supplémentaire.

Sections

- Comprendre et visualiser la simultanéité
- Calcul de la simultanéité pour une fonction événementielle
- Présentation de la simultanéité réservée et de la simultanéité allouée
- Présentation de la simultanéité et des requêtes par seconde
- Quotas de simultanéité
- Configuration de la simultanéité réservée pour une fonction événementielle
- Configuration de la simultanéité provisionnée pour une fonction événementielle
- Comportement de dimensionnement des fonctions d'événement
- Surveillance de la simultanéité

Comprendre et visualiser la simultanéité

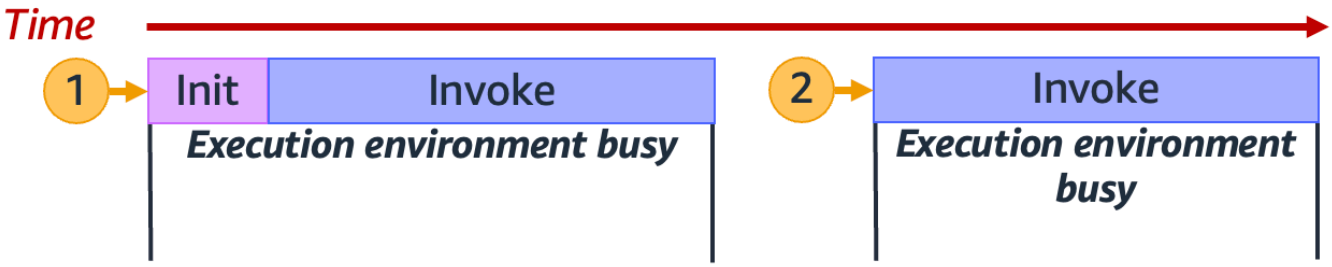
Lambda invoque votre fonction d'événement dans un environnement d'exécution sécurisé et isolé. Pour traiter une demande, Lambda doit d'abord initialiser un environnement d'exécution (phase d'initialisation), avant de l'utiliser pour appeler votre fonction d'événement (phase d'appel) :



> **Note**
>
> Les durées réelles d'initialisation et d'invocation peuvent varier en fonction de nombreux facteurs, tels que le temps d'exécution que vous choisissez et le code de la fonction d'événement Lambda. Le diagramme précédent n'est pas censé représenter les proportions exactes des durées des phases Init et Invoke.

Le diagramme précédent utilise un rectangle pour représenter un seul environnement d'exécution. Lorsque votre fonction d'événement reçoit sa toute première requête (représentée par le cercle jaune avec étiquette1), Lambda crée un nouvel environnement d'exécution et exécute le code en dehors de votre gestionnaire principal pendant la phase d'initialisation. Lambda exécute ensuite le code du gestionnaire principal de votre fonction d'événement pendant la phase d'Invoke. Pendant tout ce processus, cet environnement d'exécution est occupé et ne peut pas traiter d'autres demandes.

Lorsque Lambda a terminé de traiter la première demande, cet environnement d'exécution peut alors traiter des demandes supplémentaires pour la même fonction d'événement. Pour les demandes suivantes, Lambda n'a pas besoin de réinitialiser l'environnement.

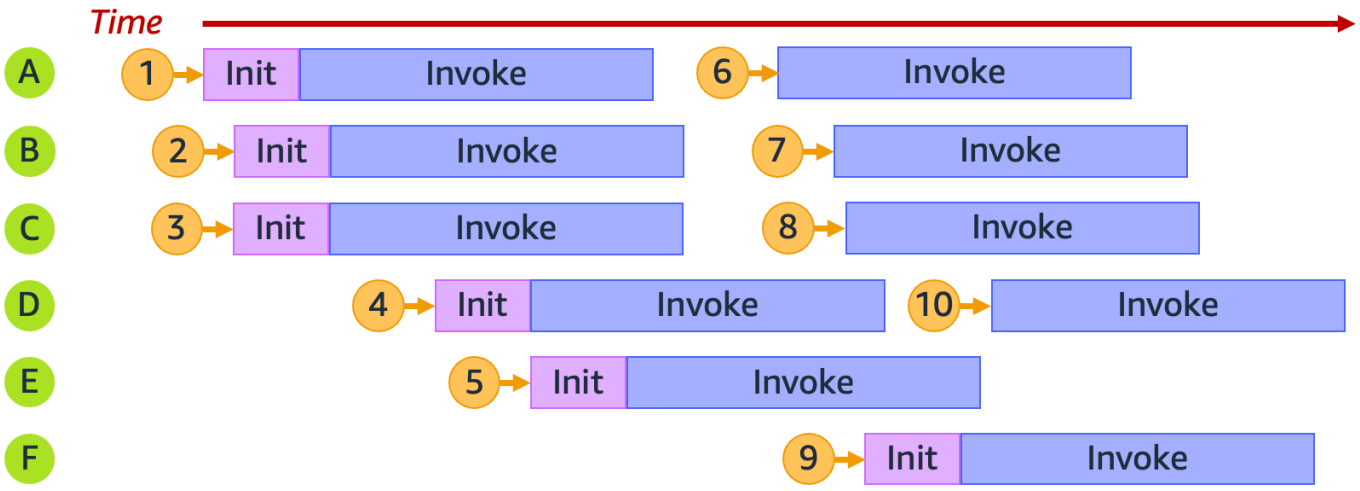


Dans le schéma précédent, Lambda réutilise l'environnement d'exécution pour traiter la deuxième demande (représentée par le cercle jaune avec l'étiquette 2).

Jusqu'à présent, nous nous sommes concentrés sur une seule instance de votre environnement d'exécution (c.-à-d. une simultanéité de 1). En pratique, Lambda peut avoir besoin de provisionner plusieurs instances d'environnement d'exécution en parallèle pour gérer toutes les demandes entrantes. Lorsque votre fonction événementielle reçoit une nouvelle demande, l'une des deux choses suivantes peut se produire :

- Si une instance d'environnement d'exécution pré-initialisée est disponible, Lambda l'utilise pour traiter la demande.
- Sinon, Lambda crée une nouvelle instance d'environnement d'exécution pour traiter la demande.

Par exemple, examinons ce qui se passe lorsque votre fonction événementielle reçoit 10 requêtes :

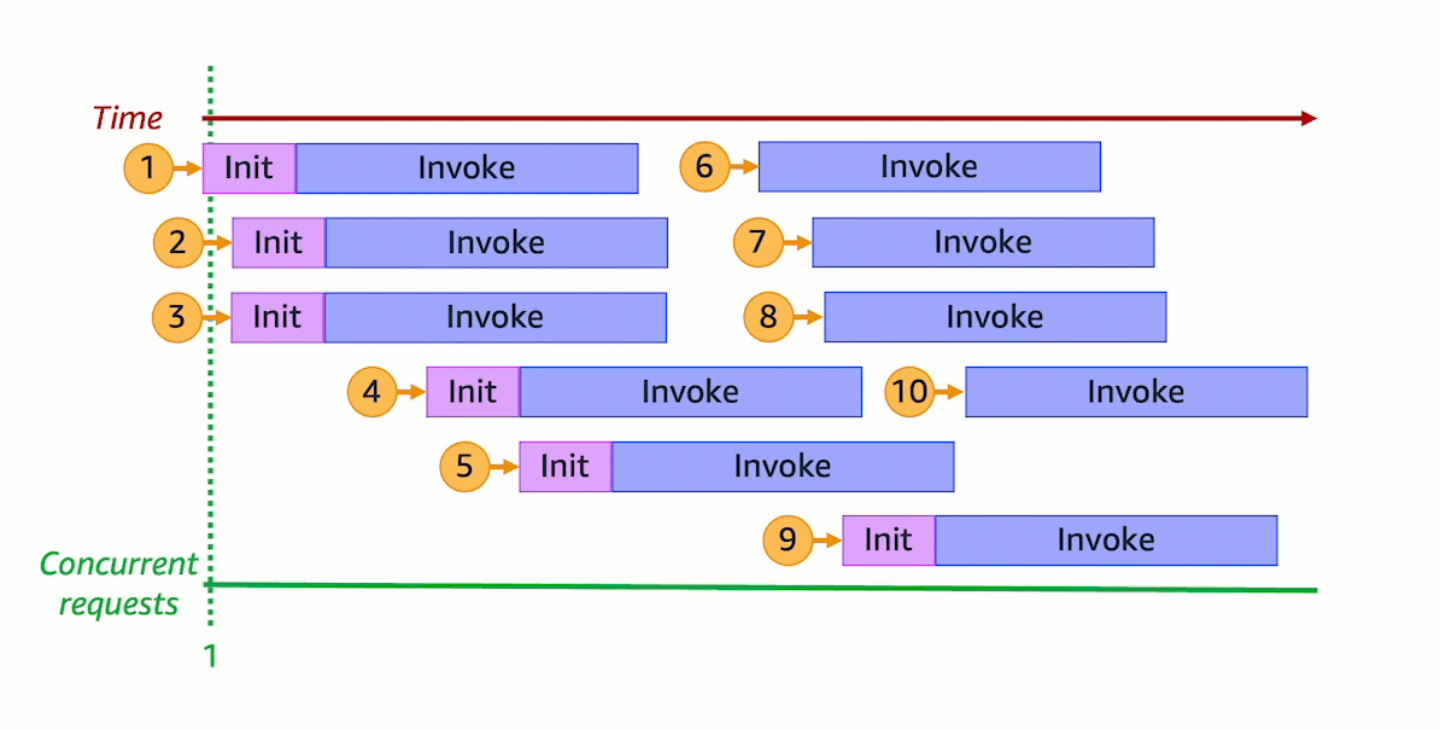


Dans le diagramme précédent, chaque plan horizontal représente une seule instance d'environnement d'exécution (étiquetée de A à F). Voici comment Lambda traite chaque demande :

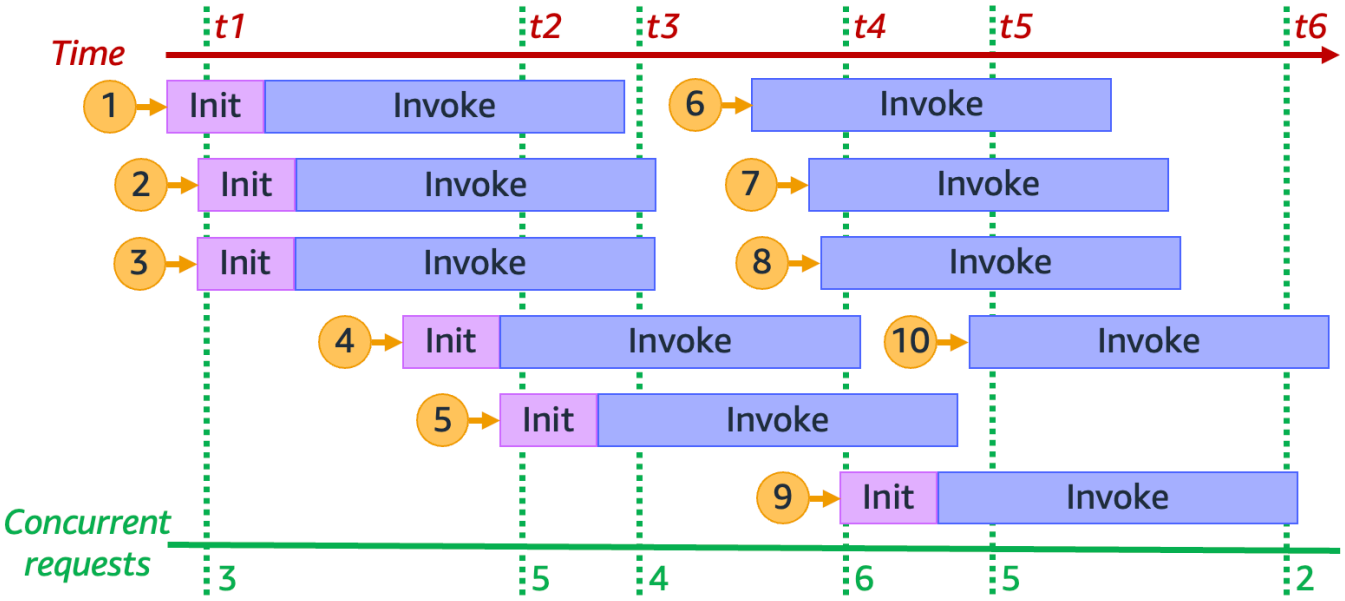
Demande	Comportement de Lambda	Raisonnement
1	Alloue un nouvel environnement A	C’est la première demande ; aucune instance d’environnement d’exécution n’est disponible.
2	Alloue un nouvel environnement B	L’instance A de l’environnement d’exécution existant est occupée.
3	Alloue un nouvel environnement C	Les instances d’environnement d’exécution existantes A et B sont toutes deux occupées.
4	Alloue un nouvel environnement D	Les instances d’environnement d’exécution existantes A, B et C sont toutes occupées.
5	Alloue un nouvel environnement E	Les instances A, B, C et D de l’environnement d’exécution existant sont toutes occupées.
6	Réutilise l’environnement A	L’instance d’environnement d’exécution A a fini de traiter la demande 1 et est maintenant disponible.
7	Réutilise l’environnement B	L’instance d’environnement d’exécution B a fini de traiter la demande 2 et est maintenant disponible.
8	Réutilise l’environnement C	L’instance d’environnement d’exécution C a terminé le

Demande	Comportement de Lambda	Raisonnement
		traitement de la demande 3 et est maintenant disponible.
9	Alloue un nouvel environnement F	Les instances d'environnement d'exécution existantes A, B, C, D et E sont toutes occupées.
10	Réutilise l'environnement D	L'instance d'environnement d'exécution D a fini de traiter la demande 4 et est maintenant disponible.

Au fur et à mesure que votre fonction d'événement reçoit de plus en plus de demandes simultanées, Lambda augmente le nombre d'instances d'environnement d'exécution en réponse. L'animation suivante suit le nombre de demandes simultanées dans le temps :



En figeant l'animation précédente à six points distincts dans le temps, nous obtenons le diagramme suivant :



Dans le diagramme précédent, nous pouvons tracer une ligne verticale à tout moment et compter le nombre d'environnements qui croisent cette ligne. Cela nous donne le nombre de demandes simultanées à ce moment précis. Par exemple, au moment `t1`, il y a trois environnements actifs servant trois demandes simultanées. Le nombre maximum de demandes simultanées dans cette simulation se produit au moment `t4`, lorsqu'il y a six environnements actifs servant six demandes simultanées.

En résumé, la simultanéité de votre fonction d'événement est le nombre de demandes simultanées qu'elle traite en même temps. En réponse à une augmentation de la simultanéité de votre fonction d'événement, Lambda fournit davantage d'instances d'environnement d'exécution pour répondre à la demande de demande.

Calcul de la simultanéité pour une fonction événementielle

En général, la simultanéité d'un système est la capacité de traiter plus d'une tâche simultanément. Dans Lambda, la simultanéité est le nombre de demandes en cours de vol traitées simultanément par votre fonction d'événement. Un moyen rapide et pratique de mesurer la simultanéité d'une fonction d'événement Lambda consiste à utiliser la formule suivante :

```
Concurrency = (average requests per second) * (average request duration in seconds)
```

La simultanéité diffère des demandes par seconde. Supposons, par exemple, que votre fonction événementielle reçoive 100 demandes par seconde en moyenne. Si la durée moyenne des demandes est de une seconde, il est vrai que la simultanéité est également de 100 :

```
Concurrency = (100 requests/second) * (1 second/request) = 100
```

Toutefois, si la durée moyenne des demandes est de 500 ms, la simultanéité est de 50 :

```
Concurrency = (100 requests/second) * (0.5 second/request) = 50
```

Que signifie une simultanéité de 50 dans la pratique ? Si la durée moyenne des demandes est de 500 ms, vous pouvez considérer qu'une instance de votre fonction est capable de traiter deux demandes par seconde. Ensuite, il faut 50 instances de votre fonction pour gérer une charge de 100 demandes par seconde. Une simultanéité de 50 signifie que Lambda doit fournir 50 instances d'environnement d'exécution pour gérer efficacement cette charge de travail sans être limité. Voici comment exprimer cela sous forme d'équation :

```
Concurrency = (100 requests/second) / (2 requests/second) = 50
```

Si votre fonction événementielle reçoit le double du nombre de demandes (200 demandes par seconde), mais ne nécessite que la moitié du temps pour traiter chaque demande (250 ms), la simultanéité est toujours de 50 :

```
Concurrency = (200 requests/second) * (0.25 second/request) = 50
```

Testez de votre compréhension de la simultanéité

Supposons que vous disposiez d'une fonction d'événement dont l'exécution prend en moyenne 200 ms. Pendant les pics de charge, vous observez 5 000 demandes par seconde. Quelle est la simultanéité de votre fonction événementielle en période de pointe ?

Réponse

La durée moyenne de la fonction d'événement est de 200 ms, soit 0,2 seconde. En utilisant la formule de simultanéité, vous pouvez entrer les chiffres pour obtenir une simultanéité de 1000 :

```
Concurrency = (5,000 requests/second) * (0.2 seconds/request) = 1,000
```

Par ailleurs, une durée moyenne d'une fonction d'événement de 200 ms signifie que votre fonction d'événement peut traiter 5 demandes par seconde. Pour traiter la charge de travail de 5 000 demandes par seconde, vous avez besoin de 1 000 instances d’environnement d’exécution. La simultanéité est donc de 1 000 :

```
Concurrency = (5,000 requests/second) / (5 requests/second) = 1,000
```

Présentation de la simultanéité réservée et de la simultanéité allouée

Par défaut, votre compte dispose d'une limite de 1 000 exécutions simultanées pour toutes les fonctions événementielles d'une région. Vos fonctions événementielles partagent ce pool de 1 000 simultanés à la demande. Vos fonctions événementielles sont limitées (c'est-à-dire qu'elles commencent à supprimer les demandes) si vous n'avez plus de simultanéité disponible.

Certaines de vos fonctions événementielles peuvent être plus critiques que d'autres. Par conséquent, vous souhaiterez peut-être configurer les paramètres de simultanéité pour garantir que les fonctions événementielles critiques obtiennent la simultanéité dont elles ont besoin. Il existe deux types de contrôles de simultanéité : la simultanéité réservée et la simultanéité provisionnée.

- Utilisez la simultanéité réservée pour définir le nombre maximum et minimum d'instances simultanées afin de réserver une partie de la simultanéité de votre compte à une fonction événementielle. Cela est utile si vous ne souhaitez pas que d'autres fonctions événementielles utilisent toutes les fonctionnalités simultanées non réservées disponibles. Lorsqu'une fonction événementielle a réservé la simultanéité, aucune autre fonction événementielle ne peut utiliser cette simultanéité.
- Utilisez la simultanéité provisionnée pour pré-initialiser un certain nombre d'instances d'environnement pour une fonction d'événement. Ceci est utile pour réduire les latences de démarrage à froid.

Simultanéité réservée

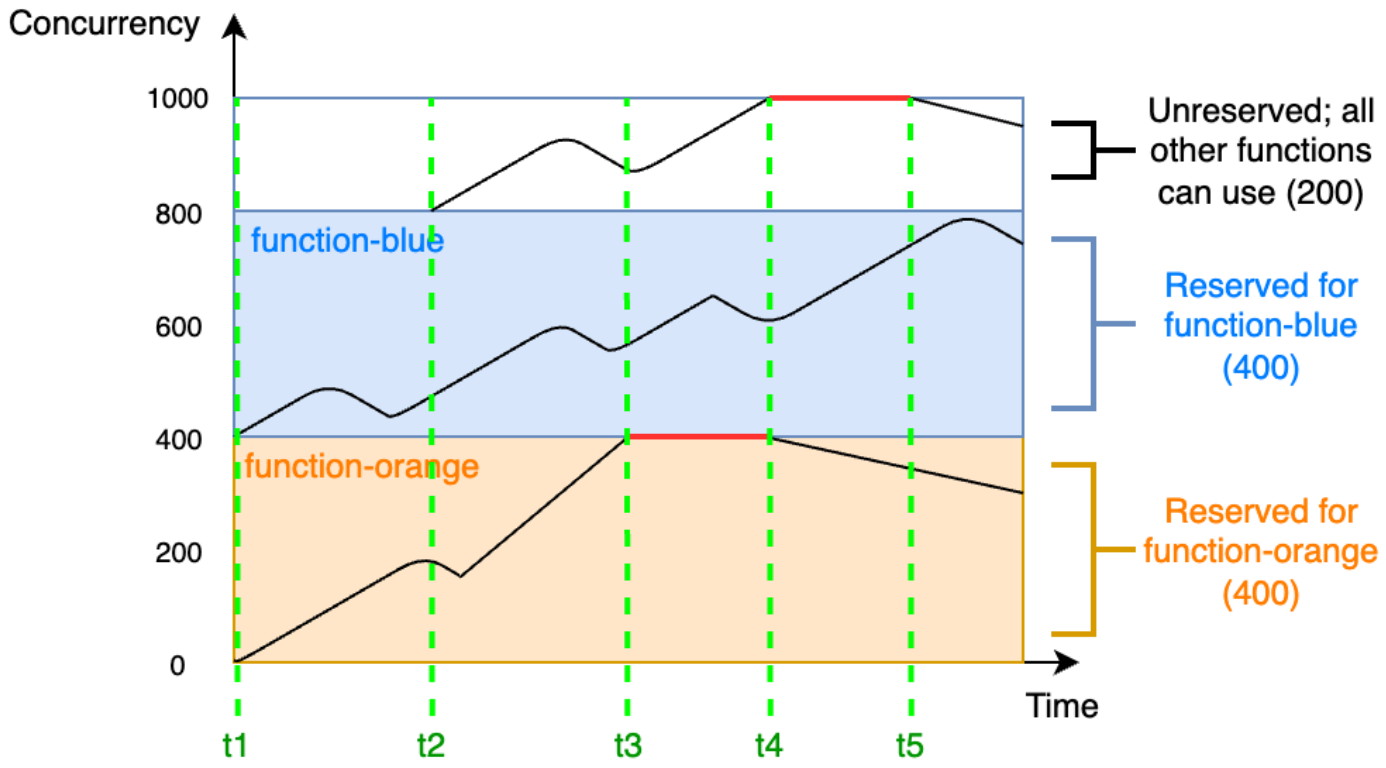
Si vous souhaitez garantir qu'un certain niveau de simultanéité est disponible pour votre fonction événementielle à tout moment, utilisez la simultanéité réservée.

La simultanéité réservée définit le nombre maximum et minimum d'instances simultanées que vous souhaitez allouer à votre fonction événementielle. Lorsque vous dédiez une simultanéité réservée à une fonction d'événement, aucune autre fonction d'événement ne peut utiliser cette simultanéité. En d'autres termes, la définition de la simultanéité réservée peut avoir un impact sur le pool de

simultanéité disponible pour les autres fonctions événementielles. Les fonctions événementielles qui n'ont pas de simultanéité réservée partagent le pool restant de simultanéité non réservée.

La configuration de la simultanéité réservée compte dans la limite globale de simultanéité de votre compte. La configuration de la simultanéité réservée pour une fonction événementielle est gratuite.

Pour mieux comprendre la simultanéité réservée, considérez le diagramme suivant :



Dans ce schéma, la limite de simultanéité de votre compte pour toutes les fonctions événementielles de cette région est fixée à la limite par défaut de 1 000. Supposons que vous disposiez de deux fonctions d'événement critiques qui s'attendent régulièrement à recevoir des volumes d'invocation élevés. `function-blue` `function-orange` Vous décidez d'accorder 400 unités de simultanéité réservée à `function-blue`, et 400 unités de simultanéité réservée à `function-orange`. Dans cet exemple, toutes les autres fonctions événementielles de votre compte doivent partager les 200 unités de simultanéité non réservées restantes.

Le diagramme présente cinq points d'intérêt :

- À `t1`, `function-orange` et `function-blue` commencent à recevoir des demandes. Chaque fonction événementielle commence à utiliser la portion allouée d'unités de simultanéité réservées.

- À `t2`, `function-orange` et `function-blue` reçoivent de plus en plus de demandes. Dans le même temps, vous déployez d'autres fonctions d'événement Lambda, qui commencent à recevoir des demandes. Vous n'attribuez pas de simultanéité réservée à ces autres fonctions événementielles. Elles commencent à utiliser les 200 unités restantes de simultanéité non réservée.
- À `t3`, `function-orange` atteint la simultanéité maximale de 400. Bien qu'il existe une simultanéité non utilisée ailleurs dans le compte, `function-orange` ne peut pas y accéder. La ligne rouge indique qu'il `function-orange` y a un ralentissement et que Lambda peut abandonner les demandes.
- À `t4`, `function-orange` commence à recevoir moins de demandes et n'est plus limitée. Cependant, vos autres fonctions événementielles connaissent un pic de trafic et commencent à s'accélérer. Bien que la simultanéité ne soit pas utilisée ailleurs dans votre compte, ces autres fonctions événementielles ne peuvent pas y accéder. La ligne rouge indique que vos autres fonctions événementielles sont soumises à un ralentissement.
- À`t5`, les autres fonctions événementielles commencent à recevoir moins de demandes et ne sont plus limitées.

À partir de cet exemple, remarquez que la réservation de la simultanéité a les effets suivants :

- Votre fonction événementielle peut évoluer indépendamment des autres fonctions événementielles de votre compte. Toutes les fonctions événementielles de votre compte dans la même région qui ne proposent pas de simultanéité réservée partagent le pool de fonctionnalités simultanées non réservées. Sans simultanéité réservée, les autres fonctions événementielles peuvent potentiellement utiliser toute la simultanéité disponible. Cela empêche les fonctions événementielles critiques de s'étendre si nécessaire.
- Votre fonction événementielle ne peut pas évoluer de manière incontrôlable. La simultanéité réservée limite la simultanéité maximale et minimale de votre fonction événementielle. Cela signifie que votre fonction événementielle ne peut pas utiliser la simultanéité réservée aux autres fonctions événementielles, ni la simultanéité provenant du pool non réservé. En outre, la simultanéité réservée agit à la fois comme une limite inférieure et une limite supérieure : elle réserve la capacité spécifiée exclusivement à votre fonction événementielle tout en l'empêchant de dépasser cette limite. Vous pouvez réserver la simultanéité pour empêcher votre fonction événementielle d'utiliser toute la simultanéité disponible sur votre compte ou de surcharger les ressources en aval.
- Il se peut que vous ne puissiez pas utiliser toutes les fonctionnalités simultanées disponibles de votre compte. La réservation de simultanéité est prise en compte dans le calcul de la

limite de simultanéité de votre compte, mais cela signifie également que les autres fonctions événementielles ne peuvent pas utiliser cette partie de la simultanéité réservée. Si votre fonction événementielle n'utilise pas toute la simultanéité que vous lui réservez, vous gaspillez cette simultanéité. Ce n'est pas un problème, sauf si d'autres fonctions événementielles de votre compte peuvent bénéficier de cette simultanéité inutile.

Pour savoir comment gérer les paramètres de simultanéité réservés pour vos fonctions événementielles, consultezConfiguration de la simultanéité réservée pour une fonction événementielle.

Simultanéité allouée

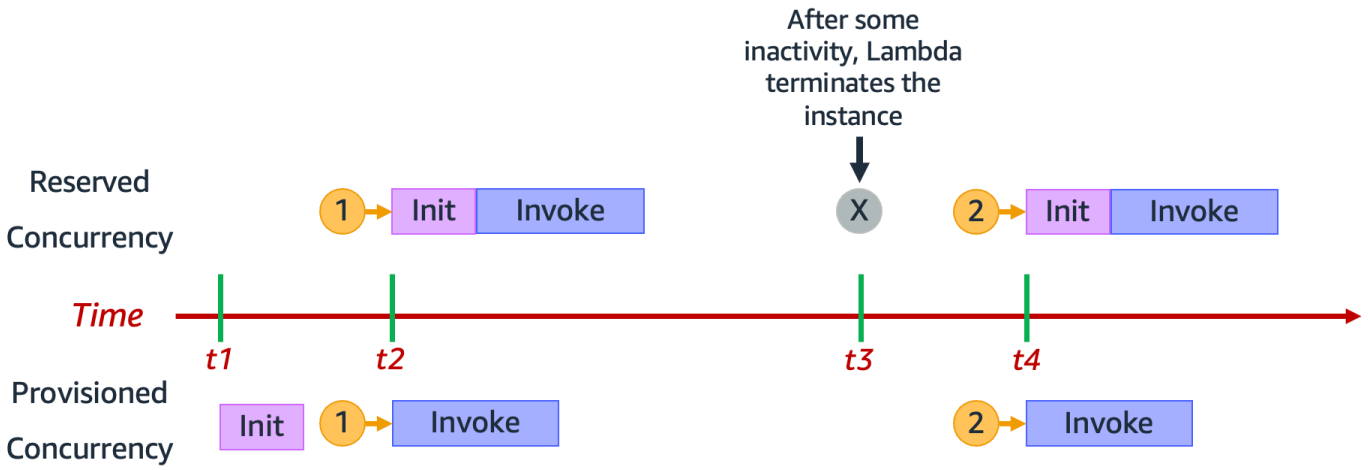
Vous utilisez la simultanéité réservée pour définir le nombre maximum d'environnements d'exécution réservés à une fonction d'événement Lambda. Toutefois, aucun de ces environnements n'est préinitialisé. Par conséquent, vos appels de fonction d'événement peuvent prendre plus de temps car Lambda doit d'abord initialiser le nouvel environnement avant de pouvoir l'utiliser pour appeler votre fonction d'événement. Lorsque Lambda doit initialiser un nouvel environnement pour effectuer un appel, cela s'appelle un démarrage à froid. Pour atténuer les démarrages à froid, vous pouvez utiliser la simultanéité provisionnée.

La simultanéité provisionnée est le nombre d'environnements d'exécution préinitialisés que vous souhaitez allouer à votre fonction événementielle. Si vous définissez la simultanéité provisionnée pour une fonction d'événement, Lambda initialise ce nombre d'environnements d'exécution afin qu'ils soient prêts à répondre immédiatement aux demandes de fonction d'événement.

> **Note**
>
> L'utilisation de la simultanéité provisionnée entraîne des frais supplémentaires sur votre compte. Si vous travaillez avec les environnements d'exécution Java 11 ou Java 17, vous pouvez également utiliser SnapStart Lambda pour atténuer les problèmes de démarrage à froid sans frais supplémentaires. SnapStart utilise des instantanés mis en cache de votre environnement d'exécution pour améliorer de manière significative les performances de démarrage. Vous ne pouvez pas utiliser les deux SnapStart et la simultanéité provisionnée sur la même version de Event Function. Pour plus d'informations sur les SnapStart fonctionnalités, les limitations et les régions prises en charge, consultezAméliorer les performances de démarrage avec Lambda SnapStart.

Lorsque vous utilisez la simultanéité provisionnée, Lambda recycle toujours les environnements d'exécution en arrière-plan. Par exemple, cela peut se produire après un échec d'invocation. Cependant, à tout moment, Lambda s'assure toujours que le nombre d'environnements pré-initialisés est égal à la valeur du paramètre de simultanéité provisionné de votre fonction d'événement. Il est important de noter que même si vous utilisez la simultanéité provisionnée, vous pourriez toujours rencontrer un retard de démarrage à froid si Lambda doit réinitialiser l'environnement d'exécution.

En revanche, lors de l'utilisation de la simultanéité réservée, Lambda peut complètement mettre fin à un environnement après une période d'inactivité. Le schéma suivant illustre cela en comparant le cycle de vie d'un environnement d'exécution unique lorsque vous configurez votre fonction d'événement en utilisant la simultanéité réservée par rapport à la simultanéité provisionnée.

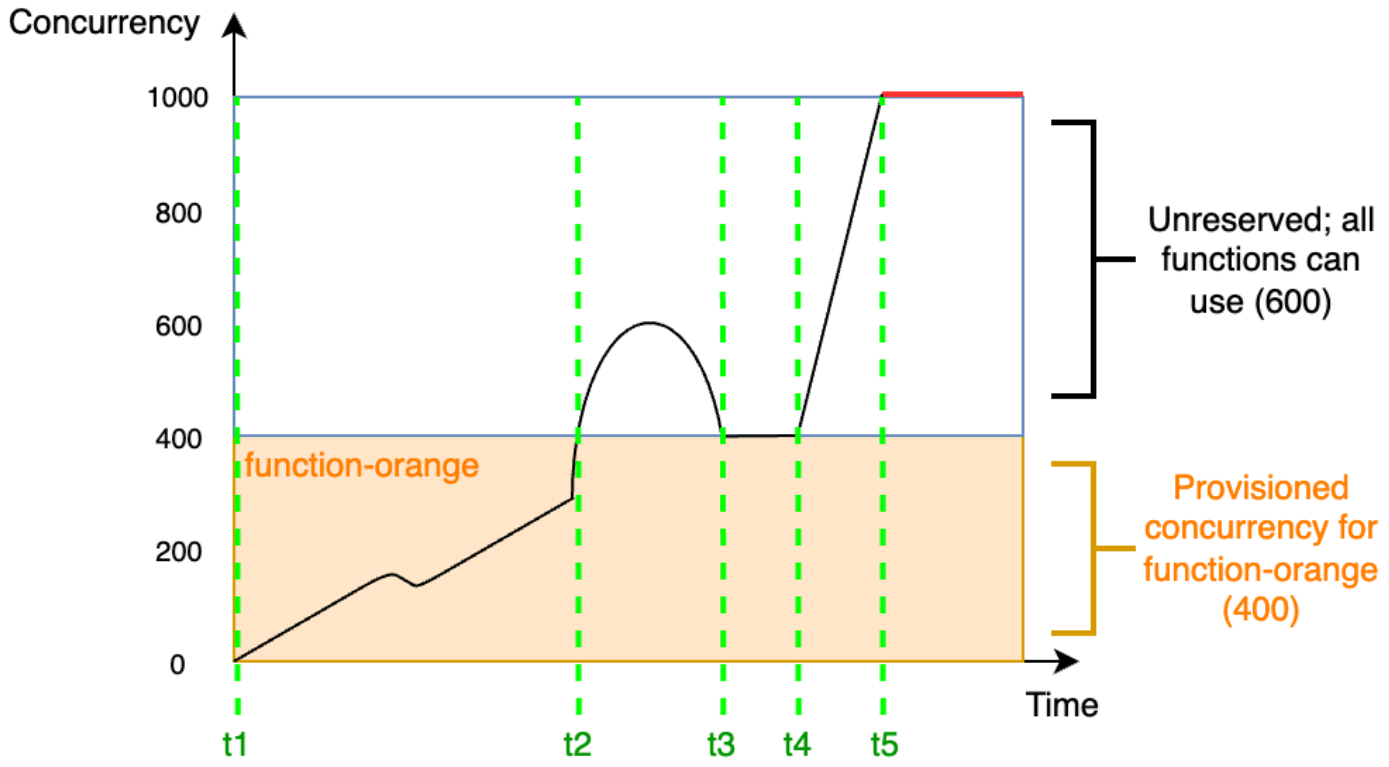


Le diagramme présente quatre points d'intérêt :

Heure	Simultanéité réservée	Simultanéité allouée
t1	Rien ne se passe.	Lambda pré-initialise une instance d'environnement d'exécution.
t2	La demande 1 arrive. Lambda doit initialiser une nouvelle instance d'environnement d'exécution.	La demande 1 arrive. Lambda utilise l'instance d'environ nement pré-initialisée.
t3	Après un certain temps d'inactivité, Lambda met fin	Rien ne se passe.

Heure	Simultanéité réservée	Simultanéité allouée
	à l'instance d'environnement active.	
t4	La demande 2 arrive. Lambda doit initialiser une nouvelle instance d'environnement d'exécution.	La demande 2 arrive. Lambda utilise l'instance d'environ nement pré-initialisée.

Pour mieux comprendre la simultanéité provisionnée, considérez le diagramme suivant :

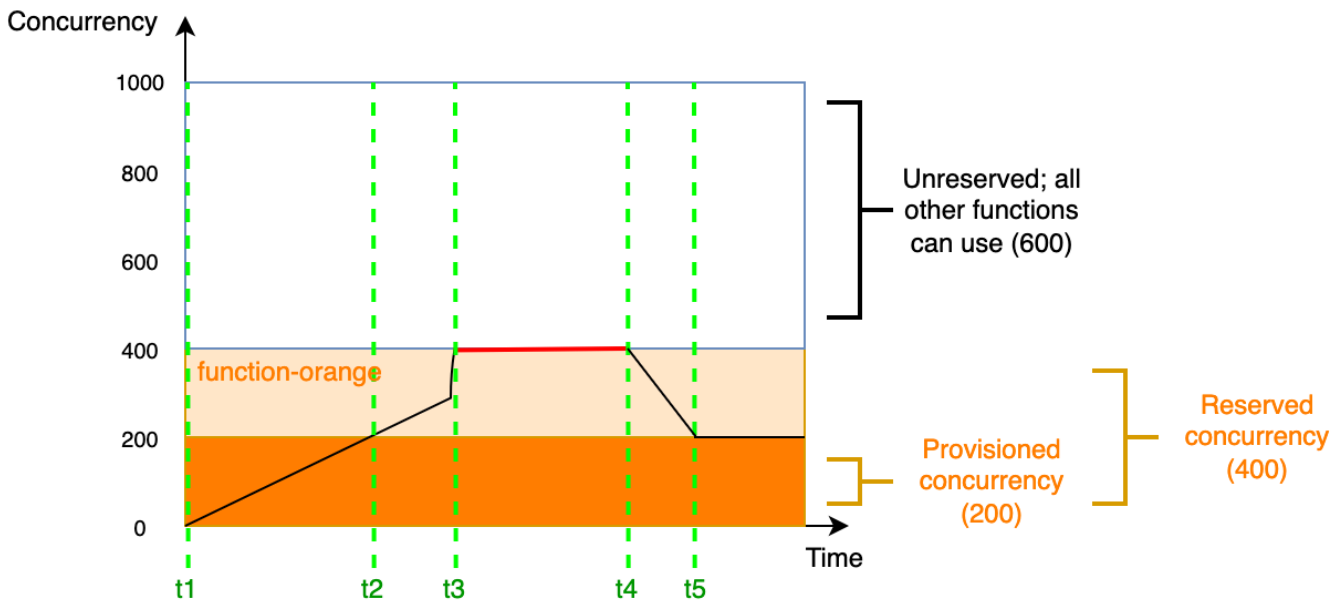


Dans ce diagramme, vous avez une limite de simultanéité de compte de 1 000. Vous décidez d'accorder 400 unités de simultanéité provisionnée à `function-orange`. Toutes les fonctions événementielles de votre compte, y compris`function-orange`, peuvent utiliser les 600 unités de simultanéité non réservées restantes.

Le diagramme présente cinq points d'intérêt :

- À `t1`, `function-orange` commence à recevoir des demandes. Puisque Lambda a pré-initialisé 400 instances d'environnement d'exécution, `function-orange` est prête pour une invocation immédiat.
- À `t2`, `function-orange` atteint 400 demandes simultanées. Par conséquent, `function-orange` n'a plus de simultanéité provisionnée. Cependant, comme il reste de la simultanéité non réservée, Lambda peut l'utiliser pour traiter des demandes supplémentaires vers `function-orange` (il n'y a pas de limitation). Lambda doit créer de nouvelles instances pour répondre à ces demandes, et votre fonction d'événement peut rencontrer des latences de démarrage à froid.
- À `t3`, `function-orange` revient à 400 demandes simultanées après un bref pic de trafic. Lambda est à nouveau capable de traiter toutes les demandes sans latence de démarrage à froid.
- Chez`t4`, les fonctions événementielles de votre compte connaissent une augmentation du trafic. Cette rafale peut provenir de votre compte `function-orange` ou de toute autre fonction événementielle. Lambda utilise la simultanéité sans réserve pour traiter ces demandes.
- À`t5`, les fonctions événementielles de votre compte atteignent la limite maximale de 1 000 simultanées et l'expérience est limitée.

L'exemple précédent ne prenait en compte que la simultanéité provisionnée. Dans la pratique, vous pouvez définir à la fois la simultanéité provisionnée et la simultanéité réservée sur une fonction événementielle. Vous pourriez le faire si vous disposiez d'une fonction événementielle qui gère un nombre constant d'appels en semaine, mais qui enregistre régulièrement des pics de trafic le week-end. Dans ce cas, vous pourriez utiliser la simultanéité provisionnée pour définir une quantité de base d'environnements pour traiter les demandes pendant les jours de la semaine, et utiliser la simultanéité réservée pour gérer les pics de trafic du week-end. Considérez le diagramme suivant :



Dans ce diagramme, supposons que vous configurez 200 unités de simultanéité provisionnée et 400 unités de simultanéité réservée pour `function-orange`. Parce que vous avez configuré la simultanéité réservée, `function-orange` ne peut utiliser aucune des 600 unités de simultanéité non réservée.

Ce diagramme comporte cinq points d'intérêt :

- À `t1`, `function-orange` commence à recevoir des demandes. Puisque Lambda a pré-initialisé 200 instances d'environnement d'exécution, `function-orange` est prête pour une invocation immédiat.
- Att2, `function-orange` utilise toute sa simultanéité provisionnée. `function-orange`peut continuer à traiter les demandes en utilisant la simultanéité réservée, mais ces demandes peuvent être confrontées à des latences de démarrage à froid.
- À `t3`, `function-orange` atteint 400 demandes simultanées. Par conséquent, `function-orange` utilise toute sa simultanéité réservée. Comme `function-orange` ne peut pas utiliser la simultanéité non réservée, les demandes commencent à être limitées.
- À `t4`, `function-orange` commence à recevoir moins de demandes et ne se limite plus.
- À `t5`, `function-orange` tombe à 200 demandes simultanées, de sorte que toutes les demandes peuvent à nouveau utiliser la simultanéité provisionnée (c.-à-d. sans latence de démarrage à froid).

La simultanéité réservée et la simultanéité provisionnée comptent toutes deux dans la limite de simultanéité de votre compte et dans les quotas régionaux. En d'autres termes, l'allocation d'une simultanéité réservée et provisionnée peut avoir un impact sur le pool de simultanéité disponible pour les autres fonctions événementielles. La configuration de la simultanéité provisionnée entraîne des frais pour votre. Compte AWS

> **Note**
>
> Si le niveau de simultanéité provisionné sur les versions et les alias d'une fonction événementielle s'ajoute à la simultanéité réservée de la fonction événementielle, toutes les invocations sont exécutées sur la base de la simultanéité provisionnée. Cette configuration a également pour effet de limiter la version non publiée de la fonction d'événement (`$LATEST`), ce qui empêche son exécution. Vous ne pouvez pas allouer plus de simultanéité provisionnée que de simultanéité réservée pour une fonction événementielle.

Pour gérer les paramètres de simultanéité configurés pour vos fonctions événementielles, consultez. Configuration de la simultanéité provisionnée pour une fonction événementielle Pour automatiser la mise à l'échelle de la concurrence provisionnée en fonction d'une planification ou de l'utilisation de l'application, consultez Utilisation d'Application Auto Scaling pour automatiser la gestion de la simultanéité provisionnée.

Comment Lambda alloue la simultanéité provisionnée

La simultanéité provisionnée n'est pas mise en ligne immédiatement après la configuration. Lambda commence à allouer la simultanéité approvisionnée après une phase de préparation d'une ou deux minutes. Pour chaque fonction événementielle, Lambda peut provisionner jusqu'à 6 000 environnements d'exécution par minute, quel que soit le cas. Région AWS C'est exactement le même que le taux de mise à l'échelle de la simultanéité pour les fonctions événementielles.

Lorsque vous soumettez une demande d'allocation de simultanéité provisionnée, vous ne pouvez accéder à aucun de ces environnements tant que Lambda n'a pas terminé de les allouer. Par exemple, si vous demandez 5 000 simultanéités allouées, aucune de vos requêtes ne peut utiliser la simultanéité allouée avant que Lambda termine l'allocation des 5 000 environnements d'exécution.

Comparaison de la simultanéité réservée et de la simultanéité provisionnée

Le tableau suivant résume et compare la simultanéité réservée et provisionnée.

Rubrique	Simultanéité réservée	Simultanéité allouée
Définition	Nombre maximum d'instances d'environnement d'exécution pour votre fonction événement ielle.	Définissez le nombre d'instanc es d'environnement d'exécuti on préprovisionnées pour votre fonction événementielle.
Comportement de provision nement	Lambda provisionne de nouvelles instances sur une base à la demande.	Lambda préapprovisionne les instances (c'est-à-dire avant que votre fonction d'événeme nt ne commence à recevoir des demandes).
Comportement de démarrage à froid	Latence de démarrage à froid possible, puisque Lambda doit créer de nouvelles instances à la demande.	Latence de démarrage à froid impossible, puisque Lambda ne doit pas créer d’instances à la demande.
Comportement de limitation	La fonction d'événement est limitée lorsque la limite de simultanéité réservée est atteinte.	Si la simultanéité réservée n'est pas définie : Event Function utilise la simultanéité non réservée lorsque la limite de simultanéité allouée est atteinte. Si la simultanéité réservée est définie : la fonction d'événeme nt est limitée lorsque la limite de simultanéité réservée est atteinte.
Comportement par défaut si non défini	Event Function utilise la simultanéité non réservée disponible sur votre compte.	Lambda ne pré-provisionne pas d’instances. En revanche, si la simultanéité réservée n'est pas définie : Event Function utilise la simultanéité non réservée disponible sur votre compte.

Rubrique	Simultanéité réservée	Simultanéité allouée
		Si la simultanéité réservée est définie : Event Function utilise la simultanéité réservée.
Tarification	Pas de frais supplémentaires.	Entraîne des frais supplémentaires.

Présentation de la simultanéité et des requêtes par seconde

Comme indiqué dans la section précédente, la simultanéité diffère des demandes par seconde. Il s'agit d'une distinction particulièrement importante à faire lorsque vous travaillez avec des fonctions d'événement dont la durée moyenne des requêtes est inférieure à 100 ms.

Pour toutes les fonctions événementielles de votre compte, Lambda applique une limite de demandes par seconde égale à 10 fois le nombre de demandes simultanées de votre compte. Par exemple, étant donné que la limite de simultanéité par défaut est de 1 000, les fonctions d'événement de votre compte peuvent traiter un maximum de 10 000 demandes par seconde.

Prenons l'exemple d'une fonction d'événement dont la durée de requête moyenne est de 50 ms. À 20 000 requêtes par seconde, voici la simultanéité de cette fonction d'événement :

```
Concurrency = (20,000 requests/second) * (0.05 second/request) = 1,000
```

Sur la base de ce résultat, vous pouvez vous attendre à ce que la limite de simultanéité de compte de 1 000 soit suffisante pour gérer cette charge. Toutefois, en raison de la limite de 10 000 demandes par seconde, votre fonction événementielle ne peut traiter que 10 000 demandes par seconde sur un total de 20 000 demandes. Cette fonction événementielle subit un ralentissement.

La leçon à tirer est que vous devez tenir compte à la fois de la simultanéité et des demandes par seconde lorsque vous configurez les paramètres de simultanéité pour vos fonctions événementielles. Dans ce cas, vous devez demander une augmentation de la limite de simultanéité des comptes à 2 000, car cela porterait le nombre total de requêtes par seconde à 20 000.

> **Note**
>
> Sur la base de cette limite de requêtes par seconde, il est faux de dire que chaque environnement d'exécution Lambda ne peut traiter qu'un maximum de 10 requêtes par

seconde. Au lieu d'observer la charge sur un environnement d'exécution individuel, Lambda ne prend en compte que la simultanéité globale et le nombre total de requêtes par seconde lors du calcul de vos quotas.

Testez votre compréhension de la simultanéité (fonctions d'événement inférieures à 100 ms)

Supposons que vous disposiez d'une fonction d'événement dont l'exécution prend en moyenne 20 ms. Pendant les pics de charge, vous observez 30 000 requêtes par seconde. Quelle est la simultanéité de votre fonction événementielle en période de pointe ?

Réponse

La durée moyenne de la fonction d'événement est de 20 ms, soit 0,02 seconde. En utilisant la formule de simultanéité, vous pouvez entrer les chiffres pour obtenir une simultanéité de 600 :

```
Concurrency = (30,000 requests/second) * (0.02 seconds/request) = 600
```

Par défaut, la limite de simultanéité de compte de 1 000 semble suffisante pour gérer cette charge. Cependant, la limite de 10 000 requêtes par seconde n'est pas suffisante pour traiter les 30 000 requêtes entrantes par seconde. Pour répondre pleinement aux 30 000 requêtes, vous devez demander une augmentation de la limite de simultanéité des comptes à 3 000 ou plus.

La limite de requêtes par seconde s'applique à tous les quotas de Lambda impliquant une simultanéité. En d'autres termes, cela s'applique aux fonctions d'événement synchrones à la demande, aux fonctions d'événement qui utilisent la simultanéité provisionnée et au comportement de dimensionnement de la simultanéité. Par exemple, voici quelques scénarios dans lesquels vous devez examiner attentivement vos limites de simultanéité et de requêtes par seconde :

- Une fonction événementielle utilisant la simultanéité à la demande peut connaître une augmentation rapide de 500 demandes toutes les 10 secondes, ou de 5 000 demandes par seconde toutes les 10 secondes, selon la première éventualité.
- Supposons que vous disposiez d'une fonction événementielle dotée d'une allocation de simultanéité provisionnée de 10. Cette fonction événementielle se transforme en simultanéité à la demande après 10 demandes simultanées ou 100 demandes par seconde, selon la première éventualité.

Quotas de simultanéité

Lambda définit des quotas pour le niveau total de simultanéité que vous pouvez utiliser pour toutes les fonctions événementielles d'une région. Ces quotas existent à deux niveaux :

- Au niveau du compte, vos fonctions événementielles peuvent avoir jusqu'à 1 000 unités de simultanéité par défaut. Pour augmenter cette limite, consultez Demande d'augmentation de quota dans le Guide de l'utilisateur Service Quotas.
- Au niveau des fonctions, vous pouvez réserver jusqu'à 900 unités de simultanéité pour toutes vos fonctions événementielles par défaut. Quelle que soit la limite totale de simultanéité de votre compte, Lambda réserve toujours 100 unités de simultanéité pour vos fonctions événementielles qui ne réservent pas explicitement la simultanéité. Par exemple, si vous avez augmenté la limite de simultanéité de votre compte à 2 000, vous pouvez réserver jusqu'à 1 900 unités de simultanéité au niveau de la fonction.
- Au niveau du compte comme au niveau de la fonction, Lambda impose également une limite de requêtes par seconde égale à 10 fois le quota de simultanéité correspondant. Cela s'applique par exemple à la simultanéité au niveau du compte, aux fonctions d'événement utilisant la simultanéité à la demande, aux fonctions d'événement utilisant la simultanéité prévue et au comportement de dimensionnement de la simultanéité. Pour plus d'informations, consultez the section called "Présentation de la simultanéité et des requêtes par seconde".

Pour vérifier le quota de simultanéité actuel de votre compte, utilisez le AWS Command Line Interface (AWS CLI) pour exécuter la commande suivante :

```
aws lambda get-account-settings
```

Vous devriez voir une sortie semblable à la suivante :

```
{
    "AccountLimit": {
        "TotalCodeSize": 80530636800,
        "CodeSizeUnzipped": 262144000,
        "CodeSizeZipped": 52428800,
        "ConcurrentExecutions": 1000,
        "UnreservedConcurrentExecutions": 900
    },
    "AccountUsage": {
        "TotalCodeSize": 410759889,
```

```
        "FunctionCount": 8
    }
}
```

`ConcurrentExecutions`est votre quota de simultanéité total au niveau du compte. `UnreservedConcurrentExecutions`est le montant de simultanéité réservé que vous pouvez toujours allouer à vos fonctions événementielles.

Au fur et à mesure que votre fonction événementielle reçoit de nouvelles demandes, Lambda augmente automatiquement le nombre d'environnements d'exécution pour traiter ces demandes jusqu'à ce que votre compte atteigne son quota de simultanéité. Toutefois, pour éviter une mise à l'échelle excessive en réponse à des pics de trafic soudains, Lambda limite la rapidité avec laquelle vos fonctions peuvent être mises à l'échelle. Ce taux de mise à l'échelle simultanée est le taux maximal auquel les fonctions événementielles de votre compte peuvent évoluer en réponse à l'augmentation des demandes. (C'est-à-dire la rapidité avec laquelle Lambda peut créer de nouveaux environnements d'exécution.) Le taux d'échelonnement de la simultanéité diffère de la limite de simultanéité au niveau du compte, qui est le montant total de simultanéité disponible pour vos fonctions événementielles.

Dans chaque fonction événementielle Région AWS, votre taux de mise à l'échelle de la simultanéité est de 1 000 instances d'environnement d'exécution toutes les 10 secondes (ou 10 000 requêtes par seconde toutes les 10 secondes). En d'autres termes, toutes les 10 secondes, Lambda peut allouer au maximum 1 000 instances d'environnement d'exécution supplémentaires, ou accueillir 10 000 requêtes supplémentaires par seconde, pour chacune de vos fonctions.

En général, il n'est pas nécessaire de se soucier de cette limitation. La vitesse de mise à l'échelle de Lambda est suffisante dans la plupart des cas d'utilisation.

Il est important de noter que le taux de mise à l'échelle de la simultanéité est une limite au niveau de la fonction. Cela signifie que chaque fonction événementielle de votre compte peut évoluer indépendamment des autres fonctions événementielles.

Pour plus d'informations sur les comportements de mise à l'échelle, consultez Comportement de dimensionnement des fonctions d'événement.

Configuration de la simultanéité réservée pour une fonction événementielle

Dans Lambda, la simultanéité est le nombre de demandes en cours de traitement par votre fonction d'événement. Il existe deux types de contrôles de la simultanéité disponibles :

- Concurrence réservée — Cela définit à la fois le nombre maximum et minimum d'instances simultanées allouées à votre fonction événementielle. Lorsqu'une fonction événementielle a réservé la simultanéité, aucune autre fonction événementielle ne peut utiliser cette simultanéité. La simultanéité réservée est utile pour garantir que vos fonctions les plus critiques disposent toujours d'une simultanéité suffisante pour traiter les requêtes entrantes. En outre, la simultanéité réservée peut être utilisée pour limiter la simultanéité afin d'éviter de surcharger les ressources en aval, comme les connexions aux bases de données. La simultanéité réservée agit à la fois comme limite inférieure et supérieure : elle réserve la capacité spécifiée exclusivement à votre fonction tout en l'empêchant de dépasser cette limite. Il n'y a pas de frais supplémentaires pour la configuration de la simultanéité réservée pour une fonction.
- Concurrence provisionnée : il s'agit du nombre d'environnements d'exécution préinitialisés alloués à votre fonction événementielle. Ces environnements d'exécution sont prêts à répondre immédiatement aux demandes de fonctions entrantes. La simultanéité allouée est utile pour réduire les latences de démarrage à froid pour les fonctions et est conçue pour rendre les fonctions disponibles avec des temps de réponse de l'ordre de quelques dixaines de millisecondes. En général, ce sont les charges de travail interactives qui tirent le meilleur parti de cette fonctionnalité. Il s'agit des applications dont les utilisateurs lancent des requêtes, telles que les applications Web et mobiles, et qui sont les plus sensibles à la latence. Les charges de travail asynchrones, telles que les pipelines de traitement des données, sont souvent moins sensibles à la latence et ne nécessitent donc généralement pas de simultanéité allouée. La configuration de la simultanéité provisionnée entraîne des frais supplémentaires pour votre. Compte AWS

Cette rubrique explique comment gérer et configurer la simultanéité réservée. Pour une présentation conceptuelle de ces deux types de contrôles de simultanéité, consultez Simultanéité réservée et simultanéité provisionnée. Pour plus d'informations sur la configuration de la simultanéité provisionnée, consultez the section called "Configuration de la simultanéité provisionnée".

> **Note**
>
> Les fonctions d'événement Lambda liées à un mappage de sources d'événements Amazon MQ ont une simultanéité maximale par défaut. Pour Apache Active MQ, le nombre maximum d'instances simultanées est de 5. Pour Rabbit MQ, le nombre maximum d'instances

simultanées est de 1. La définition de la simultanéité réservée ou provisionnée pour votre fonction événementielle ne modifie pas ces limites. Pour demander une augmentation de la simultanéité maximale par défaut lors de l'utilisation d'Amazon MQ, contactez Support.

Sections

- Configuration de la simultanéité réservée
- Estimation précise de la simultanéité réservée requise pour une fonction événementielle

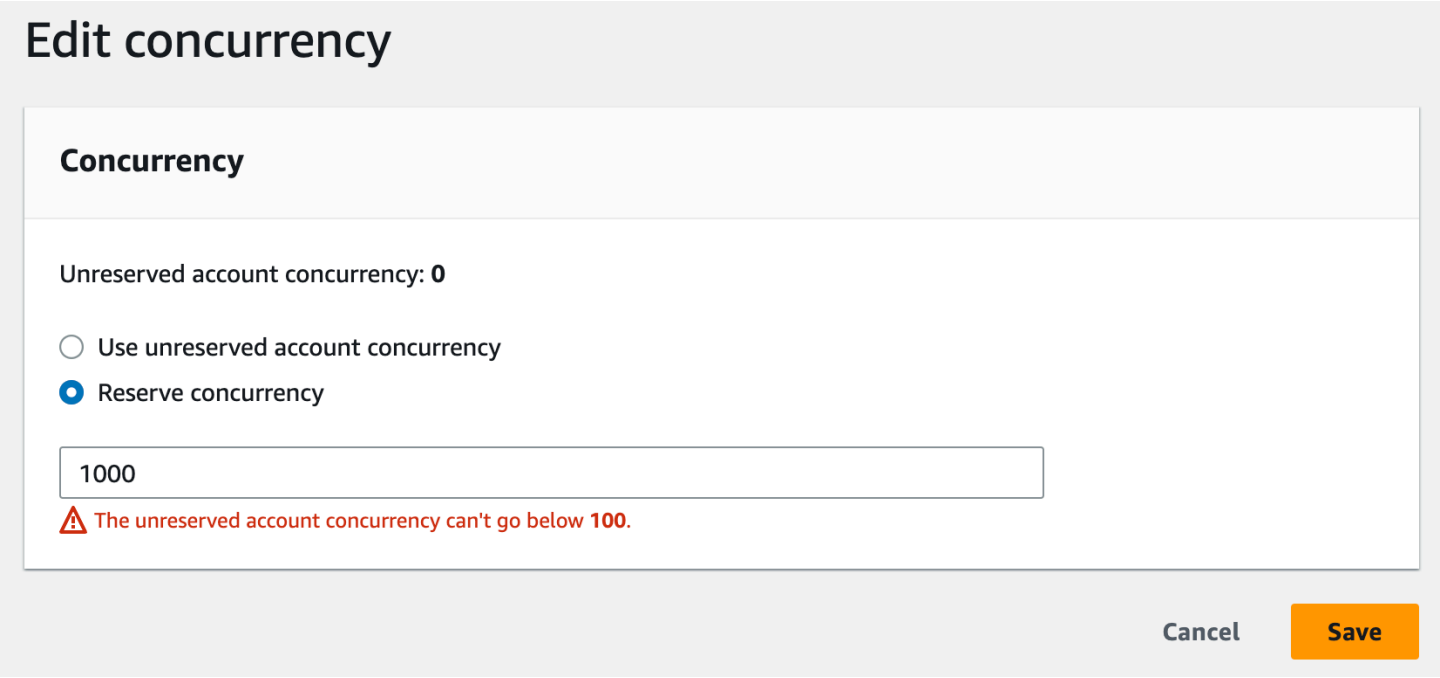
Configuration de la simultanéité réservée

Vous pouvez configurer les paramètres de simultanéité réservés pour une fonction d'événement Lambda à l'aide de la console Lambda ou de l'API Lambda.

Pour réserver la simultanéité d'une fonction événementielle (console)

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez la fonction d'événement pour laquelle vous souhaitez réserver la simultanéité.
3. Sélectionnez Configuration, puis Concurrency (Simultanéité).
4. Sous Concurrency (Simultanéité), choisissez Edit (Modifier).
5. Choisissez Reserve concurrency (Réserver la simultanéité). Entrez le montant de simultanéité à réserver pour la fonction d'événement.
6. Cliquez sur Enregistrer.

Vous pouvez réserver jusqu'à la valeur de la simultanéité du compte non réservé moins 100. Les 100 unités de simultanéité restantes concernent les fonctions événementielles qui n'utilisent pas la simultanéité réservée. Par exemple, si la limite de simultanéité de votre compte est de 1 000, vous ne pouvez pas réserver les 1 000 unités de simultanéité à une seule fonction événementielle.



La réservation de la simultanéité pour une fonction d'événement a un impact sur le pool de simultanéité disponible pour les autres fonctions d'événement. Par exemple, si vous réservez 100 unités de simultanéité pour`function-a`, les autres fonctions événementielles de votre compte doivent partager les 900 unités de simultanéité restantes, même si les 100 unités de simultanéité réservées `function-a` ne sont pas utilisées.

Pour limiter intentionnellement une fonction événementielle, définissez sa simultanéité réservée sur 0. Cela empêche votre fonction événementielle de traiter les événements jusqu'à ce que vous supprimiez la limite.

Pour configurer la simultanéité réservée avec l'API Lambda, utilisez les opérations d'API suivantes.

- PutFunctionConcurrency
- GetFunctionConcurrency
- DeleteFunctionConcurrency

Par exemple, pour configurer la simultanéité réservée avec la AWS Command Line Interface (CLI), utilisez la `put-function-concurrency` commande. La commande suivante réserve 100 unités de simultanéité pour une fonction d'événement nommée `my-function` :

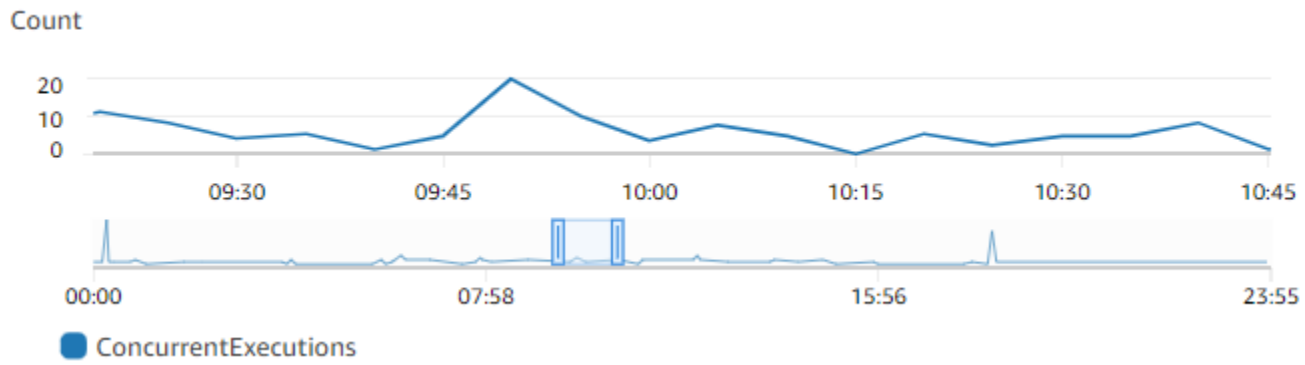
```
aws lambda put-function-concurrency --function-name my-function \
    --reserved-concurrent-executions 100
```

Vous devriez voir une sortie semblable à la suivante :

```
{
    "ReservedConcurrentExecutions": 100
}
```

Estimation précise de la simultanéité réservée requise pour une fonction événementielle

Si votre fonction événementielle gère actuellement du trafic, vous pouvez facilement consulter ses indicateurs de simultanéité à l'aide de CloudWatch métriques. Plus précisément, la `ConcurrentExecutions` métrique vous indique le nombre d'invocations simultanées pour chaque fonction événementielle de votre compte.



Le graphique précédent suggère que cette fonction d'événement répond en moyenne à 5 à 10 demandes simultanées à un moment donné, avec un pic de 20 demandes par jour normal. Supposons qu'il existe de nombreuses autres fonctions événementielles dans votre compte. Si cette fonction d'événement est essentielle à votre application et que vous ne souhaitez supprimer aucune demande, utilisez un nombre supérieur ou égal à 20 comme paramètre de simultanéité réservé.

Par ailleurs, rappelez-vous que vous pouvez également calculer la simultanéité à l'aide de la formule suivante :

```
Concurrency = (average requests per second) * (average request duration in seconds)
```

En multipliant le nombre moyen de demandes par seconde par la durée moyenne des demandes en secondes, vous obtenez une estimation approximative du niveau de simultanéité que vous devez réserver. Vous pouvez estimer les demandes moyennes par seconde à l'aide de la métrique

`Invocation`, et la durée moyenne des demandes en secondes à l'aide de la métrique `Duration`. Pour plus d'informations, consultez Utilisation de CloudWatch métriques avec Lambda.

Familiarisez-vous avec vos contraintes de débit en amont et en aval. Bien que les fonctions d'événement Lambda s'adaptent parfaitement à la charge, les dépendances en amont et en aval peuvent ne pas avoir les mêmes capacités de débit. Si vous devez limiter l'échelle de votre fonction d'événement, configurez la simultanéité réservée sur votre fonction d'événement.

Configuration de la simultanéité provisionnée pour une fonction événementielle

Dans Lambda, la simultanéité est le nombre de demandes en cours de traitement par votre fonction d'événement. Il existe deux types de contrôles de la simultanéité disponibles :

- Concurrence réservée — Cela définit à la fois le nombre maximum et minimum d'instances simultanées allouées à votre fonction événementielle. Lorsqu'une fonction événementielle a réservé la simultanéité, aucune autre fonction événementielle ne peut utiliser cette simultanéité. La simultanéité réservée est utile pour garantir que vos fonctions les plus critiques disposent toujours d'une simultanéité suffisante pour traiter les requêtes entrantes. En outre, la simultanéité réservée peut être utilisée pour limiter la simultanéité afin d'éviter de surcharger les ressources en aval, comme les connexions aux bases de données. La simultanéité réservée agit à la fois comme limite inférieure et supérieure : elle réserve la capacité spécifiée exclusivement à votre fonction tout en l'empêchant de dépasser cette limite. Il n'y a pas de frais supplémentaires pour la configuration de la simultanéité réservée pour une fonction.
- Concurrence provisionnée : il s'agit du nombre d'environnements d'exécution préinitialisés alloués à votre fonction événementielle. Ces environnements d'exécution sont prêts à répondre immédiatement aux demandes de fonctions entrantes. La simultanéité allouée est utile pour réduire les latences de démarrage à froid pour les fonctions et est conçue pour rendre les fonctions disponibles avec des temps de réponse de l'ordre de quelques dixaines de millisecondes. En général, ce sont les charges de travail interactives qui tirent le meilleur parti de cette fonctionnalité. Il s'agit des applications dont les utilisateurs lancent des requêtes, telles que les applications Web et mobiles, et qui sont les plus sensibles à la latence. Les charges de travail asynchrones, telles que les pipelines de traitement des données, sont souvent moins sensibles à la latence et ne nécessitent donc généralement pas de simultanéité allouée. La configuration de la simultanéité provisionnée entraîne des frais supplémentaires pour votre. Compte AWS

Cette rubrique explique comment gérer et configurer la simultanéité provisionnée. Pour une présentation conceptuelle de ces deux types de contrôles de simultanéité, consultez Simultanéité réservée et simultanéité provisionnée. Pour plus d'informations sur la configuration de la simultanéité réservée, consultez the section called "Configuration de la simultanéité réservée".

> **Note**
>
> Les fonctions d'événement Lambda liées à un mappage de sources d'événements Amazon MQ ont une simultanéité maximale par défaut. Pour Apache Active MQ, le nombre maximum

d'instances simultanées est de 5. Pour Rabbit MQ, le nombre maximum d'instances simultanées est de 1. La définition de la simultanéité réservée ou provisionnée pour votre fonction événementielle ne modifie pas ces limites. Pour demander une augmentation de la simultanéité maximale par défaut lors de l'utilisation d'Amazon MQ, contactez Support.

Sections

- Configuration de la simultanéité provisionnée
- Estimation précise de la simultanéité provisionnée requise pour une fonction événementielle
- Optimisation du code de la fonction d'événement lors de l'utilisation de la simultanéité provisionnée
- Utilisation de variables d'environnement pour visualiser et contrôler le comportement de simultanéité provisionnée
- Comprendre le comportement de journalisation et de facturation avec la simultanéité provisionnée
- Utilisation d'Application Auto Scaling pour automatiser la gestion de la simultanéité provisionnée

Configuration de la simultanéité provisionnée

Vous pouvez configurer les paramètres de simultanéité provisionnés pour une fonction d'événement Lambda à l'aide de la console Lambda ou de l'API Lambda.

Pour allouer la simultanéité provisionnée à une fonction événementielle (console)

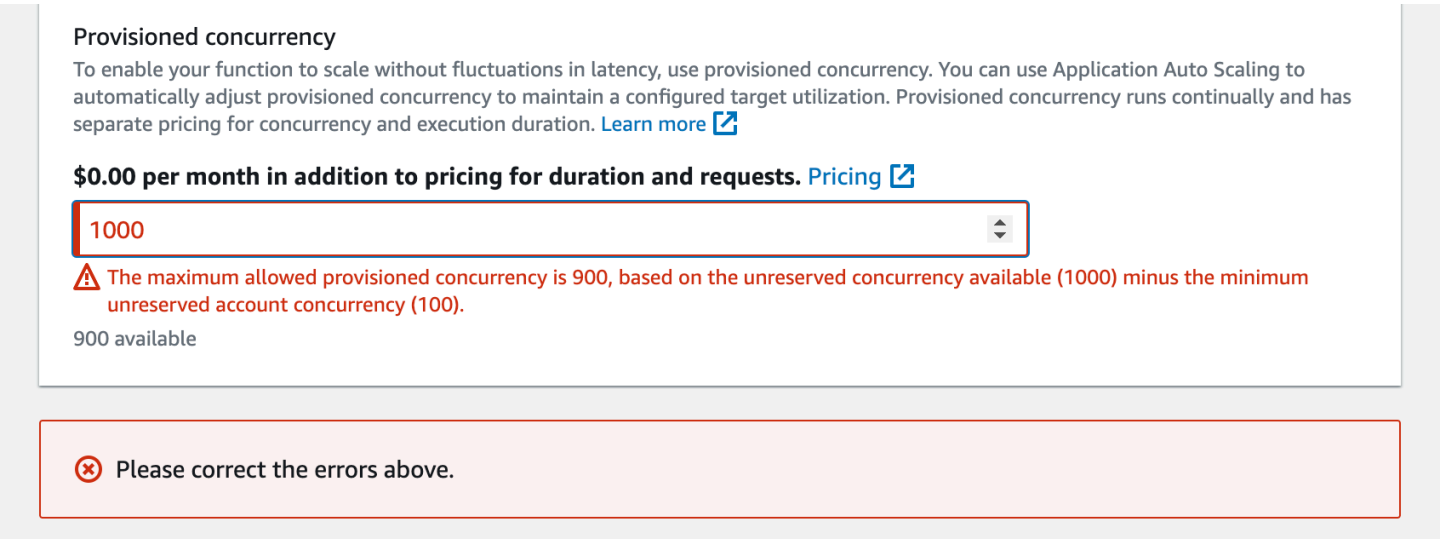
1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez la fonction d'événement pour laquelle vous souhaitez allouer la simultanéité provisionnée.
3. Sélectionnez Configuration, puis Concurrency (Simultanéité).
4. Sous Provisioned concurrency configurations (Configurations de simultanéité provisionnée), sélectionnez Add configuration (Ajouter une configuration).
5. Choisissez le type de qualificateur, ainsi que l'alias ou la version.

> **Note**
>
> Vous ne pouvez pas utiliser la simultanéité provisionnée avec la version $LATEST d'une fonction d'événement.
> Si votre fonction d'événement possède une source d'événement, assurez-vous que cette source d'événement pointe vers l'alias ou la version de fonction d'événement correct.

Dans le cas contraire, votre fonction événementielle n'utilisera pas les environnements de simultanéité provisionnés.

6. Saisissez un nombre sous Simultanéité provisionnée.
7. Cliquez sur Enregistrer.

Vous pouvez configurer jusqu'à la simultanéité du compte non réservé dans votre compte, moins 100. Les 100 unités de simultanéité restantes concernent les fonctions événementielles qui n'utilisent pas la simultanéité réservée. Par exemple, si votre compte a une limite de simultanéité de 1 000 et que vous n'avez attribué aucune simultanéité réservée ou provisionnée à aucune de vos autres fonctions événementielles, vous pouvez configurer un maximum de 900 unités de simultanéité provisionnées pour une seule fonction événementielle.



La configuration de la simultanéité provisionnée pour une fonction d'événement a un impact sur le pool de simultanéité disponible pour les autres fonctions d'événement. Par exemple, si vous configurez 100 unités de simultanéité provisionnées pour`function-a`, les autres fonctions événementielles de votre compte doivent partager les 900 unités de simultanéité restantes. Et ce même si `function-a` n'utilise pas les 100 unités.

Il est possible d'allouer à la fois une simultanéité réservée et une simultanéité provisionnée pour la même fonction événementielle. Dans de tels cas, la simultanéité provisionnée ne peut pas dépasser la simultanéité réservée.

Cette limitation s'étend aux versions de Event Function. La simultanéité allouée maximale que vous pouvez attribuer à une version spécifique de la fonction d'événement est la simultanéité réservée

de la fonction d'événement moins la simultanéité allouée sur les autres versions de la fonction d'événement.

Pour configurer la simultanéité provisionnée avec l'API Lambda, utilisez les opérations d'API suivantes.

- PutProvisionedConcurrencyConfig
- GetProvisionedConcurrencyConfig
- ListProvisionedConcurrencyConfigs
- DeleteProvisionedConcurrencyConfig

Par exemple, pour configurer la simultanéité provisionnée avec la (AWS Command Line Interface CLI), utilisez la `put-provisioned-concurrency-config` commande. La commande suivante alloue 100 unités de simultanéité provisionnée à l'BLUEalias d'une fonction d'événement nommée : `my-function`

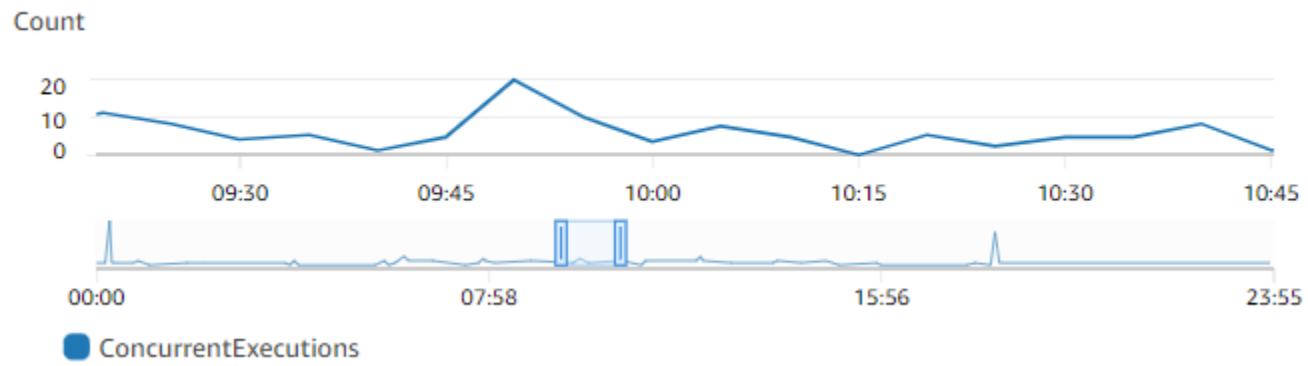
```
aws lambda put-provisioned-concurrency-config --function-name my-function \
  --qualifier BLUE \
  --provisioned-concurrent-executions 100
```

Vous devriez voir une sortie semblable à la suivante :

```
{
  "Requested ProvisionedConcurrentExecutions": 100,
  "Allocated ProvisionedConcurrentExecutions": 0,
  "Status": "IN_PROGRESS",
  "LastModified": "2023-01-21T11:30:00+0000"
}
```

Estimation précise de la simultanéité provisionnée requise pour une fonction événementielle

Vous pouvez consulter les mesures de simultanéité de n'importe quelle fonction événementielle active à l'aide de CloudWatch métriques. Plus précisément, la `ConcurrentExecutions` métrique indique le nombre d'invocations simultanées pour les fonctions événementielles dans votre compte.



Le graphique précédent suggère que cette fonction d'événement répond en moyenne à 5 à 10 demandes simultanées à un moment donné, et qu'elle atteint un pic à 20 demandes. Supposons qu'il existe de nombreuses autres fonctions événementielles dans votre compte. Si cette fonction d'événement est essentielle pour votre application et que vous avez besoin d'une réponse à faible latence à chaque appel, configurez au moins 20 unités de simultanéité provisionnées.

Rappelez-vous que vous pouvez également calculer la simultanéité à l'aide de la formule suivante :

```
Concurrency = (average requests per second) * (average request duration in seconds)
```

Pour estimer le niveau de simultanéité dont vous avez besoin, multipliez le nombre moyen de demandes par seconde par la durée moyenne des demandes en secondes. Vous pouvez estimer les demandes moyennes par seconde à l'aide de la métrique `Invocation`, et la durée moyenne des demandes en secondes à l'aide de la métrique `Duration`.

Lors de la configuration de la simultanéité provisionnée, Lambda suggère d'ajouter une mémoire tampon de 10 % en plus du niveau de simultanéité dont votre fonction événementielle a généralement besoin. Par exemple, si votre fonction événementielle atteint généralement un pic de 200 demandes simultanées, définissez la simultanéité provisionnée sur 220 (200 demandes simultanées + 10 % = 220 demandes simultanées provisionnées).

Optimisation du code de la fonction d'événement lors de l'utilisation de la simultanéité provisionnée

Si vous utilisez la simultanéité provisionnée, pensez à restructurer le code de votre fonction d'événement afin d'optimiser la faible latence. Pour les fonctions événementielles utilisant la simultanéité provisionnée, Lambda exécute n'importe quel code d'initialisation, tel que le chargement de bibliothèques et l'instanciation de clients, pendant le temps d'allocation. Par conséquent, il est conseillé de déplacer autant d'initialisation en dehors du gestionnaire de fonctions d'événement

principal pour éviter d'avoir un impact sur la latence lors des invocations de fonctions d'événement réelles. En revanche, l'initialisation de bibliothèques ou l'instanciation de clients dans le code de votre gestionnaire principal signifie que votre fonction d'événement doit l'exécuter chaque fois qu'elle est invoquée (cela se produit que vous utilisiez ou non la simultanéité provisionnée).

Pour les appels à la demande, Lambda peut avoir besoin de réexécuter votre code d'initialisation chaque fois que votre fonction d'événement démarre à froid. Pour de telles fonctions d'événement, vous pouvez choisir de différer l'initialisation d'une fonctionnalité spécifique jusqu'à ce que votre fonction d'événement en ait besoin. Par exemple, prenons le flux de contrôle suivant pour un gestionnaire Lambda :

```
def handler(event, context):
    ...
    if ( some_condition ):
        // Initialize CLIENT_A to perform a task
    else:
        // Do nothing
```

Dans l'exemple précédent, au lieu d'initialiser `CLIENT_A` en dehors du gestionnaire principal, le développeur a initialisé dans l'instruction `if`. Ainsi, Lambda n'exécute ce code que si `some_condition` est satisfaite. Si vous initialisez `CLIENT_A` en dehors du gestionnaire principal, Lambda exécute ce code à chaque démarrage à froid. Cela peut augmenter le temps de latence global.

Vous pouvez mesurer les démarrages à froid à mesure que Lambda prend de l'ampleur en ajoutant de la X-Ray surveillance à votre fonction d'événement. Une fonction événementielle utilisant la simultanéité provisionnée ne présente pas de comportement de démarrage à froid puisque l'environnement d'exécution est préparé avant l'invocation. Cependant, la simultanéité provisionnée doit être appliquée à une version ou à un alias spécifique d'une fonction d'événement, et non à la version $LATEST. Dans les cas où le comportement de démarrage à froid persiste, assurez-vous que vous invoquez la version de l'alias pour laquelle la simultanéité allouée est configurée.

Utilisation de variables d'environnement pour visualiser et contrôler le comportement de simultanéité provisionnée

Il est possible que votre fonction événementielle utilise toutes ses fonctionnalités simultanées. Lambda utilise des instances à la demande pour gérer tout trafic excédentaire. Pour déterminer quel type d'initialisation Lambda a utilisé pour un environnement particulier, vérifiez la valeur de la variable d'environnement `AWS_LAMBDA_INITIALIZATION_TYPE`.

Cette variable a deux valeurs possibles : `provisioned-concurrency` ou`on-demand`. La valeur de `AWS_LAMBDA_INITIALIZATION_TYPE` est immuable et reste constante pendant toute la durée de vie de l'environnement. Pour vérifier la valeur d'une variable d'environnement dans le code de votre fonction d'événement, consultezRécupération de variables d'environnement Lambda.

Si vous utilisez le runtime .NET 8, vous pouvez configurer la variable d'`AWS_LAMBDA_DOTNET_PREJIT`environnement pour améliorer la latence des fonctions événementielles, même si elles n'utilisent pas la simultanéité provisionnée. Le runtime .NET compile et initialise lentement chaque bibliothèque que votre code appelle pour la première fois. Par conséquent, le premier appel d'une fonction d'événement Lambda peut prendre plus de temps que les suivants. Pour atténuer ce problème, vous pouvez choisir l'une des trois valeurs `AWS_LAMBDA_DOTNET_PREJIT` :

- `ProvisionedConcurrency` : Lambda effectue une compilation JIT à l'avance pour tous les environnements utilisant la simultanéité provisionnée. C'est la valeur par défaut.
- `Always`: Lambda effectue une compilation JIT à l'avance pour chaque environnement, même si la fonction d'événement n'utilise pas la simultanéité provisionnée.
- `Never` : Lambda désactive la compilation JIT à l'avance pour tous les environnements.

Comprendre le comportement de journalisation et de facturation avec la simultanéité provisionnée

Pour les environnements de simultanéité provisionnés, le code d'initialisation de votre fonction d'événement s'exécute pendant l'allocation et régulièrement lorsque Lambda recycle les instances de votre environnement. Lambda vous facture l'initialisation même si l'instance d'environnement ne traite jamais de demande. La simultanéité provisionnée s'exécute en continu et est facturée séparément des coûts d'initialisation et d'invocation. Pour plus d'informations, consultez Tarification AWS Lambda.

Lorsque vous configurez une fonction d'événement Lambda avec une simultanéité provisionnée, Lambda pré-initialise cet environnement d'exécution afin qu'il soit disponible avant les demandes d'invocation. Lambda enregistre le champ Init Duration de la fonction d'événement dans un journal d'événements Platform-InitReport au format de journalisation JSON chaque fois que l'environnement est initialisé. Pour voir cet événement de journal, configurez votre Niveau de journal JSON sur au moins `INFO`. Vous pouvez également utiliser l'API de télémétrie pour consulter les événements de plateforme dans lesquels le champ Init Duration est indiqué.

Utilisation d'Application Auto Scaling pour automatiser la gestion de la simultanéité provisionnée

Vous pouvez utiliser Application Auto Scaling pour gérer la simultanéité provisionnée selon une planification ou en fonction de l'utilisation. Si votre fonction événementielle reçoit des modèles de trafic prévisibles, utilisez le dimensionnement planifié. Si vous souhaitez que votre fonction événementielle conserve un pourcentage d'utilisation spécifique, utilisez une politique de dimensionnement du suivi des cibles.

> **Note**
>
> Si vous utilisez Application Auto Scaling pour gérer la simultanéité provisionnée de votre fonction événementielle, assurez-vous de configurer d'abord une valeur de simultanéité provisionnée initiale. Si votre fonction d'événement ne possède pas de valeur de simultanéité initiale provisionnée, Application Auto Scaling risque de ne pas gérer correctement le dimensionnement de la fonction d'événement.

Mise à l'échelle planifiée

Avec Application Auto Scaling, vous pouvez définir votre propre planification de mise à l'échelle en fonction des changements de charge prévisibles. Pour plus d'informations et des exemples, consultez les sections Scheduled Scaling for Application Auto Scaling dans le Guide de l'utilisateur d'Application Auto Scaling et Scheduling AWS Lambda Provisioned Concurrency pour les pics d'utilisation récurrents sur le AWS Compute Blog.

Suivi des cibles

Grâce au suivi des cibles, Application Auto Scaling crée et gère un ensemble d' CloudWatch alarmes en fonction de la façon dont vous définissez votre politique de dimensionnement. Lorsque ces alarmes sont activées, Application Auto Scaling ajuste automatiquement la quantité d'environnements alloués à l'aide de la simultanéité provisionnée. Le suivi des cibles est idéal pour les applications dont les modèles de trafic ne sont pas prévisibles.

Pour mettre à l'échelle la simultanéité provisionnée à l'aide du suivi des cibles, utilisez les opérations de l'API Application Auto Scaling `RegisterScalableTarget` et `PutScalingPolicy`. Par exemple, si vous utilisez la AWS Command Line Interface (CLI), procédez comme suit :

1. Enregistrez l'alias d'une fonction événementielle en tant que cible de dimensionnement. L'exemple suivant enregistre l'alias BLUE d'une fonction d'événement nommée `my-function` :

```
aws application-autoscaling register-scalable-target --service-namespace lambda \
    --resource-id function:my-function:BLUE --min-capacity 1 --max-capacity 100 \
    --scalable-dimension lambda:function:ProvisionedConcurrency
```

2. Ensuite, appliquez une stratégie de mise à l'échelle à la cible. L'exemple suivant configure Application Auto Scaling afin d'ajuster la configuration de simultanéité provisionnée pour un alias de façon à maintenir l'utilisation proche de 70 %, mais vous pouvez appliquer n'importe quelle valeur comprise entre 10 % et 90 %.

```
aws application-autoscaling put-scaling-policy \
    --service-namespace lambda \
    --scalable-dimension lambda:function:ProvisionedConcurrency \
    --resource-id function:my-function:BLUE \
    --policy-name my-policy \
    --policy-type TargetTrackingScaling \
    --target-tracking-scaling-policy-configuration '{ "TargetValue":
 0.7, "PredefinedMetricSpecification": { "PredefinedMetricType":
 "LambdaProvisionedConcurrencyUtilization" }}'
```

Vous devriez obtenir un résultat du type suivant :

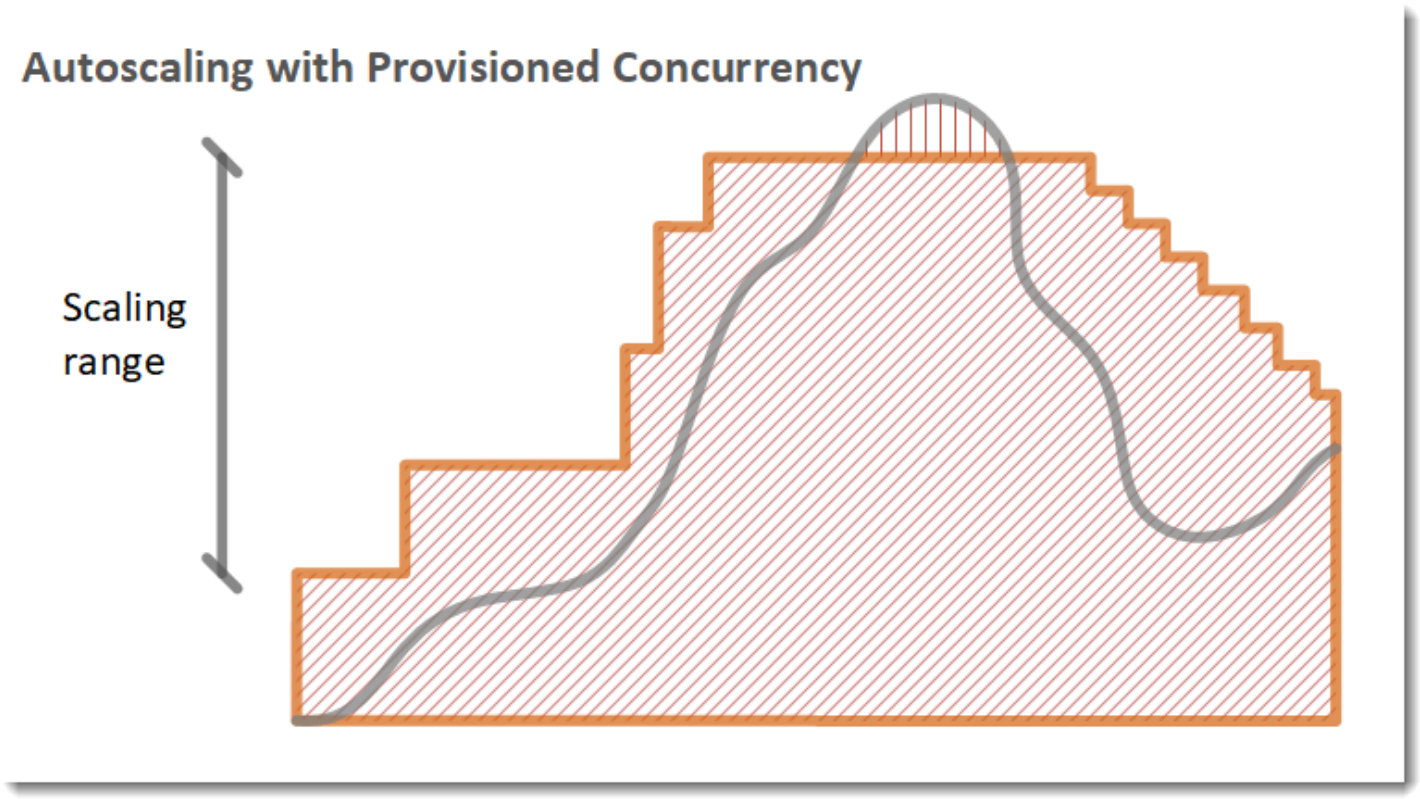
```
{
    "PolicyARN": "arn:aws:autoscaling:us-
east-2:123456789012:scalingPolicy:12266dbb-1524-xmpl-a64e-9a0a34b996fa:resource/lambda/
function:my-function:BLUE:policyName/my-policy",
    "Alarms": [
        {
            "AlarmName": "TargetTracking-function:my-function:BLUE-AlarmHigh-aed0e274-
xmpl-40fe-8cba-2e78f000c0a7",
            "AlarmARN": "arn:aws:cloudwatch:us-
east-2:123456789012:alarm:TargetTracking-function:my-function:BLUE-AlarmHigh-aed0e274-
xmpl-40fe-8cba-2e78f000c0a7"
        },
        {
            "AlarmName": "TargetTracking-function:my-function:BLUE-AlarmLow-7e1a928e-
xmpl-4d2b-8c01-782321bc6f66",
```

```
            "AlarmARN": "arn:aws:cloudwatch:us-
east-2:123456789012:alarm:TargetTracking-function:my-function:BLUE-AlarmLow-7e1a928e-
xmpl-4d2b-8c01-782321bc6f66"
        }
    ]
}
```

Application Auto Scaling crée deux alarmes dans CloudWatch. La première alarme se déclenche lorsque l'utilisation de la simultanéité provisionnée dépasse systématiquement 70 %. Lorsque cela se produit, Application Auto Scaling alloue davantage de simultanéité approvisionnée afin de réduire l'utilisation. La deuxième alarme se déclenche lorsque l'utilisation est constamment inférieure à 63 % (90 % de la cible de 70 %). Lorsque cela se produit, Application Auto Scaling réduit la simultanéité approvisionnée de l'alias.

> **Note**
>
> Lambda émet la `ProvisionedConcurrencyUtilization` métrique uniquement lorsque votre fonction d'événement est active et reçoit des demandes. Pendant les périodes d'inactivité, aucune métrique n'est émise et vos alarmes d'auto-scaling entrent dans `INSUFFICIENT_DATA` l'état. Par conséquent, Application Auto Scaling ne sera pas en mesure d'ajuster la simultanéité provisionnée de votre fonction événementielle. Cela peut entraîner une facturation imprévue.

Dans l'exemple suivant, une fonction d'événement évolue entre un minimum et un maximum de simultanéité provisionnée en fonction de l'utilisation.



Légende

- de fonctions événementielles Instanc
- Demandes ouvertes
- Simultanéité provisionnée
- Simultanéité standard

Quand le nombre de demandes ouvertes augmente, Application Auto Scaling augmente la simultanéité provisionnée par échelons jusqu'à ce qu'elle atteigne le maximum configuré. Ensuite, la fonction d'événement peut continuer à évoluer en mode de simultanéité standard et non réservée si vous n'avez pas atteint la limite de simultanéité de votre compte. Lorsque l'utilisation chute et reste constamment faible, Application Auto Scaling réduit la simultanéité provisionnée par échelons périodiques plus petits.

Les deux alarmes gérées par Application Auto Scaling utilisent la statistique moyenne par défaut. Les fonctions soumises à des pics de trafic rapides risquent de ne pas déclencher ces alarmes. Par exemple, supposons que votre fonction d'événement Lambda s'exécute rapidement (c'est-à-dire 20 à 100 ms) et que votre trafic arrive en rafales rapides. Dans ce cas, le nombre de demandes dépasse la simultanéité allouée pendant la rafale.

Cependant, Application Auto Scaling nécessite que la charge en rafale soit maintenue pendant au moins 3 minutes pour approvisionner des environnements supplémentaires. De plus, les deux CloudWatch alarmes nécessitent 3 points de données atteignant la moyenne cible pour activer la politique de dimensionnement automatique. Si votre fonction événementielle connaît des pics de trafic rapides, l'utilisation de la statistique maximale au lieu de la statistique moyenne peut être plus efficace pour étendre la simultanéité provisionnée afin de minimiser les démarrages à froid.

Pour plus d’informations sur l’utilisation des politiques de mise à l’échelle du suivi des cibles, consultez Politiques de mise à l’échelle du suivi des cibles pour Application Auto Scaling.

Comportement de dimensionnement des fonctions d'événement

Au fur et à mesure que votre fonction événementielle reçoit de nouvelles demandes, Lambda augmente automatiquement le nombre d'environnements d'exécution pour traiter ces demandes jusqu'à ce que votre compte atteigne son quota de simultanéité. Toutefois, pour éviter une mise à l'échelle excessive en réponse à des pics de trafic soudains, Lambda limite la rapidité avec laquelle vos fonctions peuvent être mises à l'échelle. Ce taux de mise à l'échelle de la simultanéité est le taux maximal auquel les fonctions événementielles de votre compte peuvent évoluer en réponse à l'augmentation du nombre de demandes. (C'est-à-dire la rapidité avec laquelle Lambda peut créer de nouveaux environnements d'exécution.) Le taux d'échelonnement de la simultanéité diffère de la limite de simultanéité au niveau du compte, qui est le montant total de simultanéité disponible pour vos fonctions événementielles.

Taux de mise à l'échelle de la simultanéité

Dans chaque Région AWS fonction événementielle et pour chaque fonction événementielle, votre taux de mise à l'échelle de la simultanéité est de 1 000 instances d'environnement d'exécution toutes les 10 secondes (ou 10 000 requêtes par seconde toutes les 10 secondes). En d'autres termes, toutes les 10 secondes, Lambda peut allouer au maximum 1 000 instances d'environnement d'exécution supplémentaires, ou accueillir 10 000 requêtes supplémentaires par seconde, pour chacune de vos fonctions.

En général, il n'est pas nécessaire de se soucier de cette limitation. La vitesse de mise à l'échelle de Lambda est suffisante dans la plupart des cas d'utilisation.

Il est important de noter que le taux de mise à l'échelle de la simultanéité est une limite au niveau de la fonction. Cela signifie que chaque fonction événementielle de votre compte peut évoluer indépendamment des autres fonctions événementielles.

> **Note**
>
> Dans la pratique, Lambda s'efforce d'augmenter votre taux de simultanéité de manière continue au fil du temps, plutôt que de procéder à une seule recharge de 1 000 unités toutes les 10 secondes.

Lambda n'accumule pas les portions inutilisées de votre taux de mise à l'échelle de la simultanéité. Cela signifie qu'à tout moment, votre taux de mise à l'échelle est toujours de 1 000 unités

simultanées au maximum. Par exemple, si vous n'utilisez aucune de vos 1 000 unités de simultanéité disponibles dans un intervalle de 10 secondes, vous n'accumulerez pas 1 000 unités supplémentaires dans le prochain intervalle de 10 secondes. Votre taux de mise à l'échelle de la simultanéité est toujours de 1 000 dans le prochain intervalle de 10 secondes.

Tant que votre fonction événementielle continue de recevoir un nombre croissant de demandes, Lambda évolue au rythme le plus rapide à votre disposition, jusqu'à la limite de simultanéité de votre compte. Vous pouvez limiter le niveau de simultanéité que les différentes fonctions événementielles peuvent utiliser en configurant la simultanéité réservée. Si les demandes arrivent plus rapidement que votre fonction événementielle ne peut être mise à l'échelle, ou si votre fonction événementielle atteint son maximum de simultanéité, les demandes supplémentaires échouent avec une erreur de régulation (code d'état 429).

Surveillance de la simultanéité

Lambda émet des métriques CloudWatch Amazon pour vous aider à surveiller la simultanéité de vos fonctions d'événement Lambda. Cette rubrique explique ces métriques et comment les interpréter.

Sections

- Métriques de simultanéité générales
- Métriques de simultanéité provisionnée
- Travailler avec la métrique ClaimedAccountConcurrency

Métriques de simultanéité générales

Utilisez les mesures suivantes pour surveiller la simultanéité de vos fonctions d'événement Lambda. La granularité de chaque métrique est d'une minute.

- `ConcurrentExecutions` : le nombre d'invocations simultanées actives à un moment donné. Lambda émet cette métrique pour toutes les fonctions d'événement, toutes les versions et tous les alias. Pour toute fonction d'événement de la console Lambda, Lambda affiche le graphique de **`ConcurrentExecutions`** manière native dans l'onglet Monitoring, sous Metrics. Consultez cette métrique en utilisant MAX.
- `UnreservedConcurrentExecutions` : le nombre d'invocations simultanées actives qui utilisent la simultanéité non réservée. Lambda émet cette métrique pour toutes les fonctions d'événement d'une région. Consultez cette métrique en utilisant MAX.
- `ClaimedAccountConcurrency` – Le niveau de simultanéité qui n'est pas disponible pour les appels à la demande. `ClaimedAccountConcurrency` est égal à `UnreservedConcurrentExecutions` plus le montant de la simultanéité allouée (c'est-à-dire le total de la simultanéité réservée plus le total de la simultanéité provisionnée). Si `ClaimedAccountConcurrency` dépasse la limite de simultanéité de votre compte, vous pouvez demander une limite de simultanéité de compte plus élevée.

  Consultez cette métrique en utilisant MAX. Pour plus d'informations, consultez Travailler avec la métrique `ClaimedAccountConcurrency`.

Métriques de simultanéité provisionnée

Utilisez les métriques suivantes pour surveiller les fonctions d'événement Lambda à l'aide de la simultanéité provisionnée. La granularité de chaque métrique est d'une minute.

- `ProvisionedConcurrentExecutions` : le nombre d'instances d'environnement d'exécution qui traitent activement une invocation sur une simultanéité allouée. Lambda émet cette métrique pour chaque version de fonction d'événement et chaque alias avec configuration de la simultanéité provisionnée. Consultez cette métrique en utilisant MAX.

`ProvisionedConcurrentExecutions` n'est pas le même que le nombre total de simultanéités provisionnées que vous allouez. Supposons, par exemple, que vous allouiez 100 unités de simultanéité provisionnée à une version de Event Function. Au cours d'une minute donnée, si au maximum 50 de ces 100 environnements d'exécution traitent des invocations simultanément, la valeur de MAX (`ProvisionedConcurrentExecutions`) est de 50.

- `ProvisionedConcurrencyInvocations`— Le nombre de fois que Lambda invoque votre code de fonction d'événement en utilisant la simultanéité provisionnée. Lambda émet cette métrique pour chaque version de fonction d'événement et chaque alias avec configuration de la simultanéité provisionnée. Consultez cette métrique en utilisant SUM.

`ProvisionedConcurrencyInvocations` diffère de `ProvisionedConcurrentExecutions`, car `ProvisionedConcurrencyInvocations` compte le nombre total d'invocations, tandis que `ProvisionedConcurrentExecutions` compte le nombre d'environnements actifs. Pour comprendre cette distinction, examinons le scénario suivant :

Dans cet exemple, supposons que vous receviez une invocation par minute et que chaque invocation dure deux minutes. Chaque barre horizontale orange représente une demande unique. Supposons que vous allouiez 10 unités de simultanéité provisionnée à cette fonction d'événement, de telle sorte que chaque demande s'exécute en cas de simultanéité provisionnée.

Entre les minutes 0 et 1, `Request 1` entre en jeu. À la minute 1, la valeur de MAX (`ProvisionedConcurrentExecutions`) est de un, puisqu'au maximum un environnement d'exécution a été actif au cours de la dernière minute. La valeur de SUM (`ProvisionedConcurrencyInvocations`) est également de un, puisqu'une nouvelle demande a été reçue au cours de la dernière minute.

Entre les minutes 1 et 2, `Request 2` entre en jeu et `Request 1` continue de fonctionner. À la minute 2, la valeur de MAX (`ProvisionedConcurrentExecutions`) est de deux, puisqu'au maximum deux environnements d'exécution ont été actifs au cours de la dernière minute. Toutefois, la valeur de SUM (`ProvisionedConcurrencyInvocations`) est de un, car une seule nouvelle demande a été reçue au cours de la dernière minute. Ce comportement métrique se poursuit jusqu'à la fin de l'exemple.

- `ProvisionedConcurrencySpilloverInvocations`— Le nombre de fois que Lambda invoque votre fonction d'événement en mode simultané standard (réservé ou non réservé) lorsque toute la simultanéité provisionnée est utilisée. Lambda émet cette métrique pour chaque version de fonction d'événement et chaque alias avec configuration de la simultanéité provisionnée. Consultez cette métrique en utilisant SUM. La valeur de `ProvisionedConcurrencyInvocations` + `ProvisionedConcurrencySpilloverInvocations` doit être égale au nombre total d'invocations de fonctions d'événement (c'est-à-dire la `Invocations` métrique).

  `ProvisionedConcurrencyUtilization` : le pourcentage de la simultanéité provisionnée utilisée (c'est à dire la valeur de `ProvisionedConcurrentExecutions` divisée par la quantité totale de la simultanéité provisionnée allouée). Lambda émet cette métrique pour chaque version de fonction d'événement et chaque alias avec configuration de la simultanéité provisionnée. Consultez cette métrique en utilisant MAX.

Supposons, par exemple, que vous fournissiez 100 unités de simultanéité provisionnée à une version de Event Function. Au cours d'une minute donnée, si au maximum 60 de ces 100 environnements d'exécution traitent des invocations simultanément, la valeur de MAX (`ProvisionedConcurrentExecutions`) est de 60 et la valeur de MAX (`ProvisionedConcurrencyUtilization`) est de 0,6.

Une valeur élevée pour `ProvisionedConcurrencySpilloverInvocations` peut indiquer que vous devez allouer une simultanéité provisionnée supplémentaire pour votre fonction événementielle. Vous pouvez également configurer Application Auto Scaling pour gérer la mise à l'échelle automatique de la simultanéité provisionnée en fonction de seuils prédéfinis.

À l'inverse, des valeurs constamment faibles pour `ProvisionedConcurrencyUtilization` peuvent indiquer que vous avez suralloué la simultanéité allouée à votre fonction événementielle.

Travailler avec la métrique **`ClaimedAccountConcurrency`**

Lambda utilise la métrique `ClaimedAccountConcurrency` pour déterminer le niveau de simultanéité disponible sur votre compte pour les appels à la demande. Lambda calcule `ClaimedAccountConcurrency` à l'aide de la formule suivante :

```
ClaimedAccountConcurrency = UnreservedConcurrentExecutions + (allocated concurrency)
```

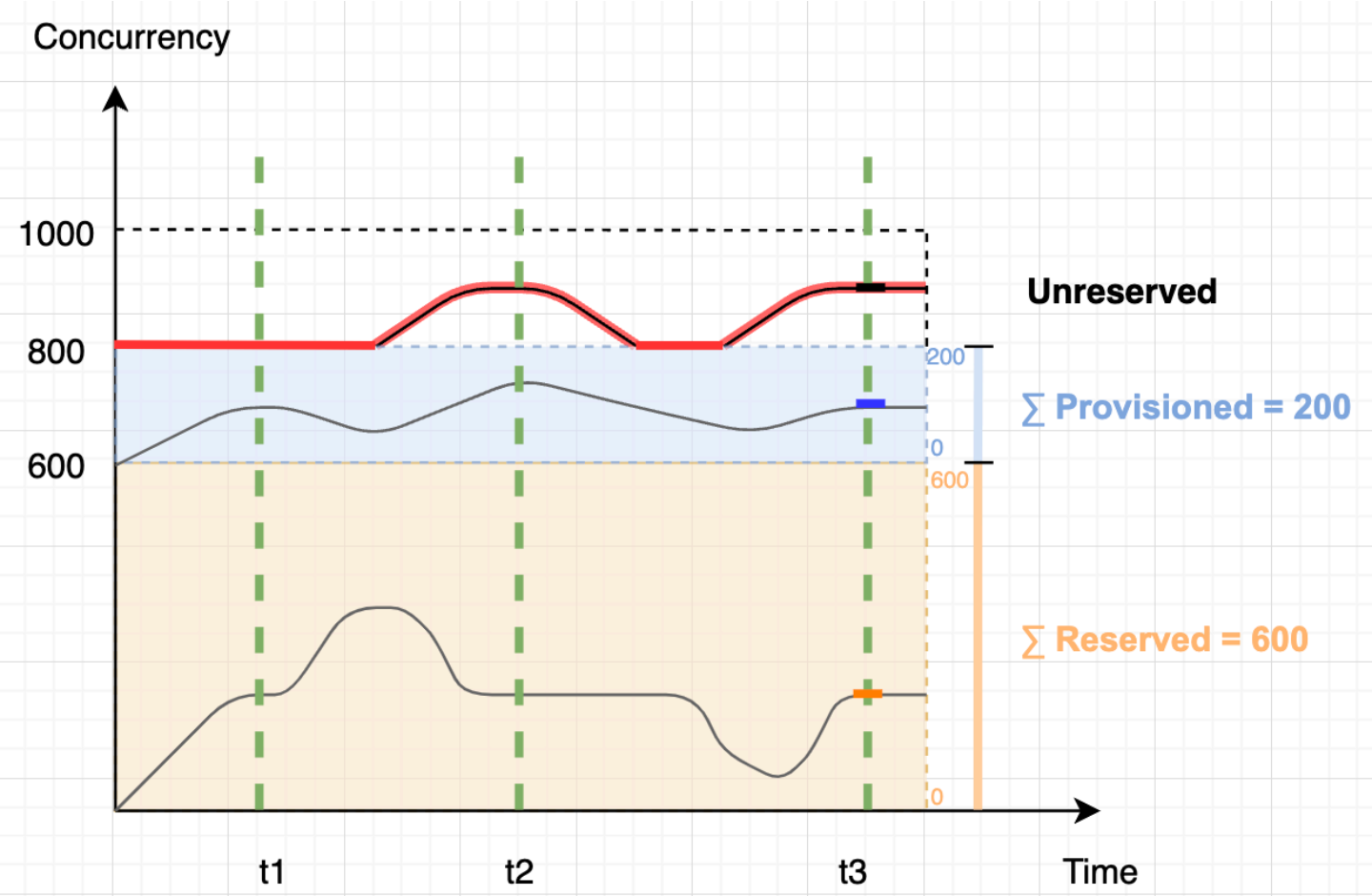
`UnreservedConcurrentExecutions` correspond au nombre d'invocations simultanées actives qui utilisent la simultanéité non réservée. La simultanéité allouée est la somme des deux parties suivantes (en les remplaçant RC en tant que « simultanéité réservée » et PC en tant que « simultanéité provisionnée ») :

- Le total de RC toutes les fonctions événementielles d'une région.
- Le total de PC toutes les fonctions événementielles d'une région qui les utilisentPC, à l'exception des fonctions événementielles qui les utilisentRC.

> **Note**
>
> Vous ne pouvez pas allouer PC plus que RC pour une fonction événementielle. Ainsi, celui d'une fonction événementielle RC est toujours supérieur ou égal à sonPC. Pour calculer la contribution à la simultanéité allouée pour de telles fonctions événementielles avec les deux PC etRC, Lambda RC ne prend en compte que le maximum des deux.

Lambda utilise la métrique `ClaimedAccountConcurrency` plutôt que `ConcurrentExecutions` pour déterminer le niveau de simultanéité disponible pour les appels à la demande. Bien que la métrique `ConcurrentExecutions` soit utile pour suivre le nombre d'appels simultanés actifs, elle ne reflète pas toujours votre véritable disponibilité simultanée. En effet, Lambda prend également en compte la simultanéité réservée et la simultanéité provisionnée pour déterminer la disponibilité.

À titre d'exemple`ClaimedAccountConcurrency`, imaginez un scénario dans lequel vous configurez une grande partie de la simultanéité réservée et de la simultanéité provisionnée entre vos fonctions événementielles qui restent largement inutilisées. Dans l'exemple suivant, supposons que la limite de simultanéité de votre compte est de 1 000 et que vous avez deux fonctions d'événement principales dans votre compte : `function-orange` et`function-blue`. Vous allouez 600 unités de simultanéité réservée pour `function-orange`. Vous allouez 200 unités de simultanéité provisionnée pour `function-blue`. Supposons qu'au fil du temps, vous déployez des fonctions d'événement supplémentaires et que vous observiez le schéma de trafic suivant :



Dans le schéma précédent, les lignes noires indiquent l'utilisation simultanée réelle au fil du temps, et la ligne rouge indique la valeur de `ClaimedAccountConcurrency` au fil du temps. Dans ce scénario, `ClaimedAccountConcurrency` c'est 800 au minimum, malgré une faible utilisation réelle de la simultanéité entre vos fonctions événementielles. Cela est dû au fait que vous avez alloué 800 unités de simultanéité au total pour `function-orange` et `function-blue`. Du point de vue de Lambda, vous avez « revendiqué » cette simultanéité pour l'utiliser, il ne vous reste donc que 200 unités de simultanéité pour les autres fonctions événementielles.

Pour ce scénario, la simultanéité allouée est de 800 dans la formule `ClaimedAccountConcurrency`. Nous pouvons ensuite déduire la valeur de `ClaimedAccountConcurrency` en différents points du diagramme :

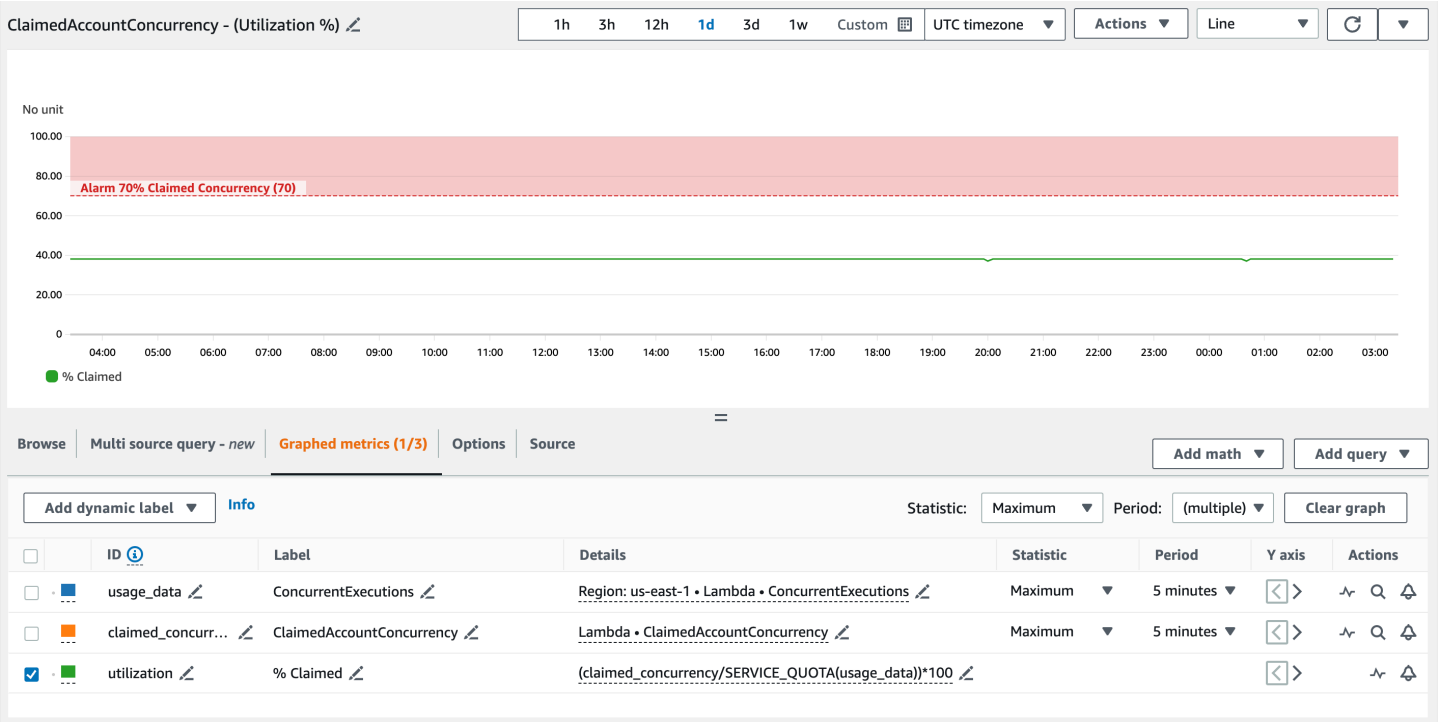
- Au niveau de `t1`, `ClaimedAccountConcurrency` est égal à 800 (800 + 0 `UnreservedConcurrentExecutions`).
- Au niveau de `t2`, `ClaimedAccountConcurrency` est égal à 900 (800 + 100 `UnreservedConcurrentExecutions`).
- Au niveau de `t3`, `ClaimedAccountConcurrency` est à nouveau égal à 900 (800 + 100 `UnreservedConcurrentExecutions`).

Configuration de la **`ClaimedAccountConcurrency`**métrique dans CloudWatch

Lambda émet la métrique en entrée. `ClaimedAccountConcurrency` CloudWatch Utilisez cette métrique avec la valeur de `SERVICE_QUOTA(ConcurrentExecutions)` pour obtenir le pourcentage d'utilisation de la simultanéité sur votre compte, comme indiqué dans la formule suivante :

```
Utilization = (ClaimedAccountConcurrency/SERVICE_QUOTA(ConcurrentExecutions)) * 100%
```

La capture d'écran suivante montre comment vous pouvez représenter graphiquement cette formule CloudWatch. La ligne verte `claim_utilization` représente l'utilisation simultanée de ce compte, qui est d'environ 40 % :



La capture d'écran précédente inclut également une CloudWatch alarme qui s'ALARMactive lorsque l'utilisation simultanée dépasse 70 %. Vous pouvez utiliser la métrique `ClaimedAccountConcurrency` ainsi que des alarmes similaires pour déterminer de manière proactive le moment où vous pourriez avoir besoin de demander une limite de simultanéité de comptes plus élevée.

Surveillance, débogage et résolution des problèmes liés aux fonctions d'événement Lambda

AWS Lambda s'intègre Services AWS à d'autres pour vous aider à surveiller et à dépanner vos fonctions d'événement Lambda. Lambda surveille automatiquement les fonctions d'événement en votre nom et publie des statistiques via Amazon. CloudWatch Pour vous aider à surveiller votre code lors de l'exécution de celui-ci, Lambda suit automatiquement le nombre de demandes, la durée d'invocation par demande et le nombre de demandes générant une erreur.

Vous pouvez utiliser other Services AWS pour résoudre les problèmes liés à vos fonctions d'événement Lambda. Cette section décrit comment les utiliser Services AWS pour surveiller, suivre, déboguer et dépanner vos fonctions et applications d'événements Lambda. Pour plus de détails sur la journalisation des fonctions d'événement et les erreurs lors de chaque exécution, consultez les sections relatives à chaque exécution. Les sujets incluent la surveillance des applications, les signaux d'application et la journalisation des appels d'API Lambda avec. CloudTrail

Sections

- Tarification
- Utilisation de CloudWatch métriques avec Lambda
- Utilisation des journaux des fonctions d'événements Lambda
- Logging AWS Lambda Appels d'API utilisant AWS CloudTrail
- Visualisez les invocations de la fonction d'événement Lambda à l'aide de AWS X-Ray
- Surveillez les performances des fonctions événementielles avec Amazon CloudWatch Lambda Insights
- Surveillance des applications Lambda
- Surveillez les performances des applications avec Amazon CloudWatch Application Signals
- Déboguer à distance les fonctions d'événement Lambda avec Visual Studio Code

Tarification

CloudWatch dispose d'un niveau gratuit perpétuel. Au-delà du seuil du niveau gratuit, les CloudWatch frais pour les métriques, les tableaux de bord, les alarmes, les journaux et les informations. Pour plus d'informations, consultez les CloudWatch tarifs Amazon.

Utilisation de CloudWatch métriques avec Lambda

Lorsque votre fonction AWS Lambda d'événement a terminé de traiter un événement, Lambda envoie automatiquement à Amazon des statistiques concernant l'invocation. CloudWatch Vous n'avez pas besoin d'accorder d'autorisations supplémentaires à votre rôle d'exécution pour recevoir les métriques Event Function, et ces mesures sont gratuites.

De nombreux types de métriques sont associés aux fonctions d'événement Lambda. Il s'agit notamment des métriques d'invocation, des métriques de performance, des métriques de simultanéité, des métriques d'invocation asynchrone et des métriques de mappage des sources d'événements. Pour plus d'informations, consultez the section called "Types de métriques".

Dans la CloudWatch console, vous pouvez consulter ces statistiques et créer des graphiques et des tableaux de bord à partir de celles-ci. Il est également possible de définir des alarmes pour réagir aux changements dans l'utilisation, les performances ou les taux d'erreur. Lambda envoie des données métriques à des intervalles d' CloudWatch une minute.

Pour un aperçu plus immédiat de votre fonction d'événement Lambda, vous pouvez créer des métriques personnalisées en haute résolution. Des frais s'appliquent pour les mesures personnalisées et les CloudWatch alarmes. Pour plus d'informations, consultez Amazon CloudWatch Pricing.

Affichage des métriques pour les fonctions d'événement Lambda

Utilisez la CloudWatch console pour consulter les métriques de vos fonctions d'événement Lambda. Dans la console, vous pouvez filtrer et trier les métriques des fonctions par nom de fonction, alias, version ou UUID de mappage des sources d'événements.

Pour afficher les métriques sur la CloudWatch console

1. Ouvrez la page Metrics (espace de `AWS/Lambda` noms) de la CloudWatch console.
2. Dans l'onglet Parcourir, sous Métriques, choisissez l'une des dimensions suivantes :

   - Par nom de fonction (`FunctionName`) : affiche les métriques agrégées pour toutes les versions et alias d'une fonction d'événement.
   - Par ressource (`Resource`) : affiche les métriques d'une version ou d'un alias d'une fonction d'événement.
   - By Executed Version (Par version exécutée) (`ExecutedVersion`) – Affichez les métriques pour une combinaison d'alias et de version. Utilisez la `ExecutedVersion` dimension pour

comparer les taux d'erreur de deux versions d'une fonction d'événement qui sont toutes deux les cibles d'un alias pondéré.

- Par UUID de mappage des sources d’événement (`EventSourceMappingUUID`) : affiche les métriques d’un mappage des sources d’événement.
- Dans toutes les fonctions (aucune) : affichez les statistiques agrégées pour toutes les fonctions événementielles actuelles Région AWS.

3. Choisissez une métrique. La métrique doit apparaître automatiquement dans le graphique visuel, ainsi que sous l’onglet Graphiques des métriques.

Par défaut, les graphiques utilisent la statistique `Sum` pour toutes les métriques. Pour choisir une autre statistique et personnaliser le graphique, utilisez les options de l'onglet Graphique des métriques.

> **Note**
>
> L'horodatage d'une métrique indique le moment où la fonction d'événement a été invoquée. En fonction de la durée de l'invocation, il peut se rapporter à plusieurs minutes avant l'émission de la métrique. Par exemple, si le délai d'expiration de votre fonction d'événement est de 10 minutes, regardez plus de 10 minutes dans le passé pour obtenir des mesures précises.

Pour plus d'informations CloudWatch, consultez le guide de CloudWatch l'utilisateur Amazon.

Types de métriques pour les fonctions d'événement Lambda

Cette section décrit les types de métriques Lambda disponibles dans la CloudWatch console.

Rubriques

- Métriques d’invocation
- Métriques de déploiement
- Métriques de performances
- Métriques de simultanéité
- Métriques d'invocations asynchrones
- Métriques de mappage des sources d’événements

Métriques d’invocation

Les métriques d'invocation sont des indicateurs binaires du résultat d'un appel de fonction d'événement Lambda. Vous devez visualiser les métriques suivantes avec la statistique `Sum`. Par exemple, si la fonction d'événement renvoie une erreur, Lambda envoie la `Errors` métrique avec une valeur de 1. Pour connaître le nombre d'erreurs liées à la fonction d'événement survenues chaque minute, `Sum` consultez la `Errors` métrique sur une période d'une minute.

- `Invocations`— Le nombre de fois que votre code de fonction d'événement est invoqué, y compris les invocations réussies et celles qui entraînent une erreur de fonction. Les invocations ne sont pas enregistrés si la demande d'invocation est limitée ou si elle entraîne une erreur d'invocation. La valeur de `Invocations` est égale au nombre de demandes facturées.
- `Errors` – Nombre d'invocations entraînant une erreur de fonction. Les erreurs de fonction incluent les exceptions levées par votre code et par l'exécution Lambda. L'environnement d'exécution renvoie des erreurs pour des problèmes tels que les expirations de délai et les erreurs de configuration. Pour calculer le taux d'erreur, divisez la valeur `Errors` par la valeur `Invocations`. Notez que l'horodatage d'une métrique d'erreur indique le moment où la fonction d'événement a été invoquée, et non le moment où l'erreur s'est produite.
- `DeadLetterErrors`— Pour un appel asynchrone, le nombre de fois que Lambda tente d'envoyer un événement vers une file d'attente de lettres mortes (DLQ) mais échoue. Dead-letter des erreurs peuvent survenir en raison de ressources mal définies ou de limites de taille.
- `DestinationDeliveryFailures` – Pour l'invocation asynchrone et les mappages des sources d'événements pris en charge, le nombre de fois où Lambda tente d'envoyer un événement à une destination, mais échoue. Pour les mappages des sources d'événements, Lambda prend en charge les destinations des sources de flux (DynamoDB et Kinesis). Des erreurs de remise peuvent se produire en raison d’erreurs d’autorisations, de ressources mal configurées ou des limites de taille. Des erreurs peuvent également se produire si la destination que vous avez configurée est un type non pris en charge, tel qu'une file d'attente FIFO Amazon SQS ou une rubrique FIFO Amazon SNS.
- `Throttles` – Nombre de demandes d'invocation limitées. Lorsque toutes les instances de fonction traitent des requêtes et qu'aucune simultanéité n'est disponible pour effectuer une augmentation, Lambda rejette les requêtes supplémentaires avec une erreur `TooManyRequestsException`. Les demandes limitées et les autres erreurs d'invocation ne comptent pas comme `Invocations` ou `Errors`.

> **Note**
>
> Avec les instances gérées Lambda, Lambda fournit des métriques d'accélération granulaires qui identifient la contrainte spécifique à l'origine de l'accélération. Lorsqu'un accélérateur se produit dans l'environnement d'exécution, exactement l'une des sous-métriques suivantes est émise avec une valeur de 1, tandis que les trois autres sont émises avec une valeur de 0. La `Throttles` métrique est toujours émise à côté de ces sous-métriques.
>
> - `CPUThrottles`— Les appels sont limités en raison de l'épuisement du processeur dans l'environnement d'exécution.
> - `MemoryThrottles`— Les appels sont limités en raison de l'épuisement de la mémoire dans l'environnement d'exécution.
> - `DiskThrottles`— Les appels sont limités en raison de l'épuisement du disque dans l'environnement d'exécution.
> - `ConcurrencyThrottles`— Les appels sont limités lorsque la limite de simultanéité de l'environnement d'exécution est atteinte.

- `OversizedRecordCount`— Pour les sources d'événements Amazon DocumentDB, le nombre d'événements que votre fonction d'événement reçoit de votre flux de modifications dont la taille est supérieure à 6 Mo. Lambda supprime le message et émet cette métrique.
- `ProvisionedConcurrencyInvocations`— Le nombre de fois que votre code de fonction d'événement est invoqué à l'aide de la simultanéité provisionnée.
- `ProvisionedConcurrencySpilloverInvocations`— Le nombre de fois que votre code de fonction d'événement est invoqué en utilisant la simultanéité standard alors que toutes les simultanités configurées sont utilisées.
- `RecursiveInvocationsDropped`— Le nombre de fois où Lambda a arrêté l'invocation de votre fonction d'événement parce qu'il a détecté que votre fonction d'événement faisait partie d'une boucle récursive infinie. La détection de boucle récursive surveille le nombre de fois qu'une fonction d'événement est invoquée dans le cadre d'une chaîne de requêtes en suivant les métadonnées ajoutées par les AWS SDK compatibles. Par défaut, si votre fonction d'événement est invoquée dans le cadre d'une chaîne de requêtes environ 16 fois, Lambda abandonne l'appel suivant. Si vous désactivez la détection des boucles récursives, cette métrique n'est pas émise. Pour en savoir plus sur cette fonction, consultez Utilisation de la détection de boucle récursive Lambda pour prévenir les boucles infinies.

Métriques de déploiement

Les métriques de déploiement fournissent des informations sur les événements de déploiement de la fonction d'événement Lambda et les processus de validation associés.

- `SignatureValidationErrors` : le nombre de fois qu'un déploiement de package de code s'est produit avec des échecs de validation de signature lorsque la politique de configuration de signature de code est définie sur `Warn`. Cette métrique est émise lorsque les vérifications d'expiration, d'incompatibilité ou de révocation échouent, mais que le déploiement est toujours autorisé en raison du paramètre de politique `Warn`. Pour plus d'informations sur la signature de code, consultez Utilisation de la signature de code pour vérifier l'intégrité du code avec Lambda.

Métriques de performances

Les indicateurs de performance fournissent des informations détaillées sur les performances d'une seule invocation d'une fonction d'événement. Par exemple, la `Duration` métrique indique le temps en millisecondes que votre fonction événementielle passe à traiter un événement. Pour avoir une idée de la rapidité avec laquelle votre fonction événementielle traite les événements, consultez ces indicateurs à l'aide de la `Max` statistique `Average` or.

- `Duration`— Le temps que votre code Event Function consacre au traitement d'un événement. La durée facturée pour une invocation est la valeur de la `Duration` arrondie à la milliseconde la plus proche. La `Duration` n'inclut pas le temps de démarrage à froid.
- `PostRuntimeExtensionsDuration`— Le temps cumulé que le moteur d'exécution passe à exécuter le code des extensions une fois le code de la fonction d'événement terminé.
- `IteratorAge` : pour les sources d'événements DynamoDB, Kinesis et Amazon DocumentDB, l'âge en millisecondes du dernier enregistrement dans l'événement. Cette métrique mesure le délai entre le moment où un flux reçoit l'enregistrement et le moment où le mappage de la source d'événement envoie l'événement à la fonction d'événement.
- `OffsetLag`— Pour les sources d'événements autogérées Apache Kafka et Amazon Managed Streaming for Apache Kafka (Amazon MSK), différence de décalage entre le dernier enregistrement écrit sur un sujet et le dernier enregistrement traité par le groupe de consommateurs de votre fonction d'événement. Bien qu'une rubrique Kafka puisse comporter plusieurs partitions, cette métrique mesure le décalage de décalage au niveau de la rubrique.

`Duration` prend également en charge les statistiques de centiles (p). Utilisez les centiles pour exclure les valeurs aberrantes qui faussent les statistiques `Average` et `Maximum`. Par exemple, la

statistique p95 indique la durée maximale de 95 % des invocations, en excluant les 5 % les plus lentes. Pour plus d'informations, consultez la section Percentiles dans le guide de CloudWatch l'utilisateur Amazon.

Métriques de simultanéité

Lambda indique les métriques de simultanéité sous la forme d'un nombre agrégé du nombre d'instances traitant des événements au sein d'une fonction d'événement, d'une version, d'un alias ou. Région AWS Pour voir la distance qui vous sépare des limites de simultanéité, affichez ces métriques à l'aide de la statistique `Max`.

- `ConcurrentExecutions`— Le nombre d'instances de fonctions événementielles qui traitent des événements. Si ce nombre atteint votre quota d'exécutions simultanées pour la région, ou la limite de simultanéité réservée pour la fonction d'événement, Lambda limite les demandes d'invocation supplémentaires.
- `ProvisionedConcurrentExecutions`— Le nombre d'instances de fonctions événementielles qui traitent des événements en utilisant la simultanéité provisionnée. Pour chaque invocation d'alias ou de version avec une simultanéité approvisionnée, Lambda émet le nombre actuel. Si votre fonction d'événement est inactive ou ne reçoit pas de demandes, Lambda n'émet pas cette métrique.
- `ProvisionedConcurrencyUtilization` : pour une version ou un alias, la valeur de `ProvisionedConcurrentExecutions` divisée par la quantité totale de simultanéité allouée configurée. Par exemple, si vous configurez une simultanéité provisionnée de 10 pour votre fonction événementielle et que votre valeur `ProvisionedConcurrentExecutions` est de 7, alors votre valeur `ProvisionedConcurrencyUtilization` est de 0,7.

  Si votre fonction d'événement est inactive ou ne reçoit pas de demandes, Lambda n'émet pas cette métrique car elle est basée sur. `ProvisionedConcurrentExecutions` Gardez cela à l'esprit si vous l'utilisez `ProvisionedConcurrencyUtilization` comme base pour les CloudWatch alarmes.
- `UnreservedConcurrentExecutions`— Pour une région, le nombre d'événements traités par Event Functions sans accès simultané réservé.
- `ClaimedAccountConcurrency` – Pour une région, le niveau de simultanéité qui n'est pas disponible pour les appels à la demande. `ClaimedAccountConcurrency` est égal à `UnreservedConcurrentExecutions` plus le montant de la simultanéité allouée (c'est-à-dire le total de la simultanéité réservée plus le total de la simultanéité provisionnée). Pour plus d'informations, consultez Travailler avec la métrique `ClaimedAccountConcurrency`.

Métriques d'invocations asynchrones

Les métriques d'invocations asynchrones fournissent des informations détaillées sur les invocations asynchrones à partir des sources d'événements et des invocations directes. Vous pouvez définir des seuils et des alarmes pour vous avertir de certaines modifications. Par exemple, en cas d'augmentation indésirable du nombre d'événements mis en file d'attente pour traitement (`AsyncEventsReceived`). Ou encore lorsqu'un événement attend depuis longtemps d'être traité (`AsyncEventAge`).

- `AsyncEventsReceived` : le nombre d'événements que Lambda met correctement en file d'attente pour traitement. Cette métrique donne un aperçu du nombre d'événements qu'une fonction d'événement reçoit. Surveillez cette métrique et définissez des alarmes pour des seuils afin de détecter les problèmes. Par exemple, pour détecter un nombre indésirable d'événements envoyés à Lambda et pour diagnostiquer rapidement les problèmes résultant de configurations de déclencheurs ou de fonctions incorrectes. Les incompatibilités entre `AsyncEventsReceived` et `Invocations` peuvent indiquer une disparité de traitement, des événements abandonnés ou un éventuel backlog dans les files d'attente.
- `AsyncEventAge`— Le délai entre le moment où Lambda met correctement l'événement en file d'attente et le moment où la fonction d'événement est invoquée. La valeur de cette métrique augmente lorsque des événements font l'objet d'une nouvelle tentative en raison d'échecs d'invocation ou de limitation. Surveillez cette métrique et définissez des alarmes pour les seuils sur différentes statistiques lorsqu'une accumulation de file d'attente se produit. Pour résoudre le problème d'une augmentation de cette métrique, examinez la métrique `Errors` pour identifier les erreurs de fonction et la métrique `Throttles` pour identifier les problèmes de simultanéité.
- `AsyncEventsDropped`— Le nombre d'événements supprimés sans que la fonction d'événement ne soit correctement exécutée. Si vous configurez une file d'attente de lettres mortes (DLQ) ou une destination `OnFailure`, les événements y sont envoyés avant d'être supprimés. Les événements sont supprimés pour diverses raisons. Par exemple, les événements peuvent dépasser l'âge maximal de l'événement ou atteindre le nombre maximal de nouvelles tentatives, ou la simultanéité réservée peut être définie sur 0. Pour déterminer pourquoi les événements sont supprimés, examinez la métrique `Errors` pour identifier les erreurs de fonction et la métrique `Throttles` pour identifier les problèmes de simultanéité.

Métriques de mappage des sources d’événements

Les métriques de mappage des sources d’événements fournissent des informations sur le comportement de traitement de votre mappage des sources d’événements.

Actuellement, les métriques de mappage des sources d'événements sont disponibles pour Amazon SQS, Kinesis, DynamoDB, Amazon MSK et les sources d'événements Apache Kafka autogérées.

Pour le mappage des sources d'événements avec la configuration des métriques, vous pouvez également vérifier toutes les métriques liées à ESM dans l'onglet Monitor depuis la page Console Lambda > Ressources supplémentaires > mappages de sources d'événements maintenant.

Pour activer des métriques ou un mappage des sources d’événements (console)

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez la fonction d'événement pour laquelle vous souhaitez activer les métriques.
3. Choisissez Configuration, puis Déclencheurs.
4. Choisissez le mappage des sources d’événements pour lequel vous souhaitez activer les métriques, puis choisissez Modifier.
5. Sous Configuration du mappage des sources d'événements, choisissez Activer les mesures ou sélectionnez-les dans la liste déroulante des mesures.
6. Cliquez sur Enregistrer.

Vous pouvez également activer les métriques pour le mappage de la source de votre événement par programmation à l'aide de l' EventSourceMappingMetricsConfigobjet contenu dans votre. EventSourceMappingConfiguration Par exemple, la commande UpdateEventSourceMappingCLI suivante active les métriques pour le mappage d'une source d'événement :

```
aws lambda update-event-source-mapping \
    --uuid a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
    --metrics-config Metrics=EventCount
```

Il existe 3 groupes de métriques :`EventCount`, `ErrorCount` et`KafkaMetrics`, et chaque groupe possède plusieurs métriques. Toutes les métriques ne sont pas disponibles pour chaque source d'événement. Le tableau suivant récapitule les mesures prises en charge pour chaque type de source d'événement.

Vous devez vous inscrire au groupe de mesures pour recevoir les mesures associées aux métriques. Par exemple, définissez EventCount dans la configuration des métriques les valeurs suivantes : (`PolledEventCount`,,`FilteredOutEventCount`,`InvokedEventCount`, `FailedInvokeEventCount`

DroppedEventCountOnFailureDestinationDeliveredEventCount, et). DeletedEventCount

Métrique de mappage des sources d'événements	Groupe de métriques	Amazon SQS	Streams Kinesis et DynamoDB	Amazon MSK et Apache Kafka autogéré
PolledEventCount	EventCount	Oui	Oui	Oui
FilteredOutEventCount	EventCount	Oui	Oui	Oui
InvokedEventCount	EventCount	Oui	Oui	Oui
FailedInvokeEventCount	EventCount	Oui	Oui	Oui
DroppedEventCount	EventCount	Non	Oui	Oui
OnFailureDestinationDeliveredEventCount	EventCount	Non	Oui	Oui
DeletedEventCount	EventCount	Oui	Non	Non
CommittedEventCount	EventCount	Non	Non	Oui
PollingErrorCount	ErrorCount	Non	Non	Oui

Métrique de mappage des sources d'événements	Groupe de métriques	Amazon SQS	Streams Kinesis et DynamoDB	Amazon MSK et Apache Kafka autogéré
`InvokeErrorCount`	`ErrorCount`	Non	Non	Oui
`OnFailureDestinationDeliveryErrorCount`	`ErrorCount`	Non	Non	Oui
`SchemaRegistryErrorCount`	`ErrorCount`	Non	Non	Oui
`CommitErrorCount`	`ErrorCount`	Non	Non	Oui
`MaxOffsetLag`	`KafkaMetrics`	Non	Non	Oui
`SumOffsetLag`	`KafkaMetrics`	Non	Non	Oui

En outre, si votre mappage des sources d'événements est en mode alloué, Lambda fournit la métrique suivante :

- `ProvisionedPollers` : pour les mappages des sources d'événements en mode alloué, le nombre de sondeurs d'événements qui s'exécutent activement. Visualisez cette métrique à l'aide des `MAX` calculs.
- (Amazon MSK et sources d'événements Apache Kafka autogérées uniquement) `EventPollerUnit` — Pour les mappages de sources d'événements en mode provisionné, le nombre d'unités d'interrogation d'événements en cours d'exécution. Visualisez cette métrique à l'aide des `SUM` calculs.

- (Amazon MSK et sources d'événements Apache Kafka autogérées) `EventPollerThroughputInBytes` — Pour les mappages de sources d'événements en mode provisionné, taille d'enregistrement totale des sondeurs d'événements interrogés à partir de la source d'événements. Il peut vous indiquer le débit d'interrogation actuel. Visualisez cette métrique à l'aide des `SUM` calculs.

Voici plus de détails sur chacune des métriques :

- `PolledEventCount` : le nombre d'événements que Lambda lit correctement depuis la source des événements. Si Lambda interroge des événements, mais reçoit un sondage vide (aucun nouvel enregistrement), Lambda émet une valeur nulle pour cette métrique. Utilisez cette métrique pour détecter si votre mappage des sources d'événements interroge correctement les nouveaux événements.
- `FilteredOutEventCount` :pour le mappage des sources d'événements avec un critère de filtre, le nombre d'événements filtrés selon ces critères de filtre. Utilisez cette métrique pour détecter si votre mappage des sources d'événements filtre correctement les événements. Pour les événements qui répondent aux critères de filtre, Lambda émet une métrique nulle.
- `InvokedEventCount`— Le nombre d'événements qui ont appelé votre fonction d'événement Lambda. Utilisez cette métrique pour vérifier que les événements invoquent correctement votre fonction d'événement. Si un événement entraîne une erreur de fonctionnement ou un ralentissement, le même événement interrogé `InvokedEventCount` peut être pris en compte plusieurs fois en raison des nouvelles tentatives automatiques.

  > **Warning**
  >
  > Les mappages des sources d'événements Lambda traitent chaque événement au moins une fois, et le traitement des enregistrements peut être dupliqué. De ce fait, les événements peuvent être comptés plusieurs fois dans les métriques impliquant le décompte des événements.

- `FailedInvokeEventCount`— Le nombre d'événements avec lesquels Lambda a essayé d'appeler votre fonction d'événement, mais qui ont échoué. Les appels peuvent échouer pour des raisons telles que des problèmes de configuration réseau, des autorisations incorrectes ou la suppression d'une fonction, d'une version ou d'un alias d'événement Lambda. Si l'option Réponse par lots partielle est activée pour votre mappage des sources d'événements,

`FailedInvokeEventCount` inclut tout événement dont la réponse contient un champ `BatchItemFailures` non vide.

> **Note**
>
> L'horodatage de la `FailedInvokeEventCount` métrique représente la fin de l'invocation de la fonction d'événement. Ce comportement est différent des autres métriques d'erreur d'appel Lambda, qui sont horodatées au début de l'appel de la fonction d'événement.

- `DroppedEventCount` : le nombre d'événements que Lambda a abandonnés en raison de l'expiration ou de l'épuisement des tentatives. Plus précisément, il s'agit du nombre d'enregistrements qui dépassent les valeurs configurées pour `MaximumRecordAgeInSeconds` ou `MaximumRetryAttempts`. Il est important de noter que cela n'inclut pas le nombre d'enregistrements qui expirent en raison du dépassement des paramètres de conservation de la source de votre événement. Les événements abandonnés excluent également les événements que vous envoyez vers une destination en cas d'échec. Utilisez cette métrique pour détecter un arriéré croissant d'événements.
- `OnFailureDestinationDeliveredEventCount` : pour les mappages des sources d'événements avec une destination en cas d'échec configurée, le nombre d'événements envoyés vers cette destination. Utilisez cette métrique pour surveiller les erreurs de fonctionnement liées aux appels provenant de cette source d'événements. Si la livraison à destination échoue, Lambda gère les métriques comme suit :
  - Lambda n'émet pas la métrique `OnFailureDestinationDeliveredEventCount`.
  - Pour la métrique `DestinationDeliveryFailures`, Lambda émet un 1.
  - Pour la métrique `DroppedEventCount`, Lambda émet un nombre égal au nombre d'événements ayant échoué à la livraison.
- `DeletedEventCount` : le nombre d'événements que Lambda a réussi à supprimer après traitement. Si Lambda échoue à la tentative de suppression d'un événement, il émet une métrique nulle. Utilisez cette métrique pour vous assurer que les événements traités avec succès sont supprimés de votre source d'événements.
- `CommittedEventCount`— Le nombre d'événements que Lambda a correctement validés après leur traitement. Il s'agit de la somme des deltas du dernier décalage validé et du décalage actuel par rapport à chaque partition dans le mappage des sources d'événements Kafka.

- `PollingErrorCount`— Le nombre d'erreurs pendant lesquelles Lambda n'a pas réussi à interroger les demandes provenant de la source de l'événement. Lambda n'émet ces données métriques qu'en cas d'erreur.
- `InvokeErrorCount`— Le nombre d'erreurs pendant lesquelles Lambda n'a pas réussi à appeler votre fonction d'événement. Notez que l'invocation est enregistrée par lots. Le numéro est indiqué au niveau du lot, et non au niveau du nombre d'enregistrements. Lambda n'émet ces données métriques qu'en cas d'erreur.
- `SchemaRegistryErrorCount`— Le nombre d'erreurs que Lambda n'a pas réussi à récupérer le schéma ou à désérialiser avec le schéma. Lambda n'émet ces données métriques qu'en cas d'erreur.
- `CommitErrorCount`— Le nombre d'erreurs que Lambda n'a pas réussi à commettre dans le cluster Kafka. Lambda n'émet ces données métriques qu'en cas d'erreur.
- `MaxOffsetLag`— Le maximum des décalages de décalage (différence entre les derniers décalages et les décalages validés) sur toutes les partitions du mappage des sources d'événements.
- `SumOffsetLag`— La somme des décalages entre toutes les partitions du mappage des sources d'événements.

Si le mappage des sources d’événements est désactivé, vous ne recevrez pas de statistiques de mappage des sources d’événements. Il est également possible que des métriques soient manquantes si CloudWatch Lambda connaît une dégradation de la disponibilité.

Utilisation des journaux des fonctions d'événements Lambda

Pour vous aider à résoudre les défaillances, surveille AWS Lambda automatiquement les fonctions d'événement Lambda en votre nom. Vous pouvez consulter les journaux des fonctions d'événements Lambda à l'aide de la console Lambda, de la console, du CloudWatch AWS Command Line Interface (AWS CLI) et de l'API. CloudWatch Vous pouvez également configurer Lambda pour envoyer les journaux à Amazon S3 et Firehose.

Tant que le rôle d'exécution de votre fonction d'événement dispose des autorisations nécessaires, Lambda capture les journaux de toutes les demandes traitées par votre fonction d'événement et les envoie à Amazon CloudWatch Logs, qui est la destination par défaut. Vous pouvez également laisser la console Lambda configurer Amazon S3 ou Firehose comme destinations de journalisation.

- CloudWatch Logs est la destination de journalisation par défaut pour les fonctions d'événements Lambda. CloudWatch Logs fournit des fonctionnalités de visualisation et d'analyse des journaux en temps réel, ainsi qu'une assistance pour créer des métriques et des alarmes basées sur les données de vos journaux.
- Amazon S3 est économique pour le stockage à long terme, et des services comme Athena peuvent être utilisés pour analyser les journaux. La latence est généralement plus élevée.
- Firehose propose une diffusion en continu gérée des journaux vers différentes destinations. Si vous devez envoyer des logs à d'autres AWS services (par exemple, OpenSearch Service ou Redshift Data API) ou à des plateformes tierces (comme Datadog, New Relic ou Splunk), Firehose simplifie ce processus en fournissant des intégrations prédéfinies. Vous pouvez également diffuser vers des points de terminaison HTTP personnalisés sans configurer d’infrastructure supplémentaire.

Choix d’une destination de service à laquelle envoyer les journaux

Tenez compte des facteurs clés suivants lorsque vous choisissez un service comme destination pour les journaux des fonctions d'événement :

- La gestion des coûts varie selon le service. Amazon S3 constitue généralement l'option la plus économique pour le stockage à long terme, tandis que CloudWatch Logs permet de consulter les journaux, de les traiter et de configurer des alertes en temps réel. Les coûts de Firehose incluent à la fois le service de diffusion en continu et le coût associé à la destination vers laquelle vous diffusez.
- Les capacités d'analyse varient d'un service à l'autre. CloudWatch Logs excelle dans la surveillance en temps réel et s'intègre nativement à d'autres CloudWatch fonctionnalités, telles

que Logs Insights et Live Tail. Amazon S3 fonctionne bien avec des outils d'analyse tels qu'Athena et peut s'intégrer à divers services, même s'il peut nécessiter une configuration supplémentaire. Firehose simplifie le streaming direct vers des AWS services spécifiques (tels que OpenSearch Service et Redshift Data API) et des plateformes tierces prises en charge (telles que Datadog et Splunk) en fournissant des intégrations prédéfinies, ce qui peut réduire le travail de configuration.

- La configuration et la facilité d'utilisation varient selon le service. CloudWatch Les journaux sont la destination par défaut des journaux. Elle fonctionne immédiatement, sans configuration supplémentaire, et permet de visualiser et d'analyser les journaux directement via la CloudWatch console. Si vous avez besoin d’envoyer les journaux à Amazon S3, vous devez effectuer une configuration initiale dans la console Lambda et configurer les autorisations du compartiment. Si vous avez besoin de journaux envoyés directement à des services tels que OpenSearch Service ou à des plateformes d'analyse tierces, Firehose peut simplifier ce processus.

Configuration des destinations de journal

AWS Lambda prend en charge plusieurs destinations pour vos journaux de fonctions événementielles. Ce guide explique les destinations de journalisation disponibles et vous aide à choisir l’option adaptée à vos besoins. Quelle que soit la destination choisie, Lambda propose des options pour contrôler le format, le filtrage et la diffusion des journaux.

Lambda prend en charge les formats JSON et texte brut pour les journaux de votre fonction d'événement. Les journaux structurés JSON offrent une meilleure facilité de recherche et permettent une analyse automatisée, tandis que les journaux en texte brut offrent une simplicité et des coûts de stockage potentiellement réduits. Vous pouvez contrôler les journaux que Lambda envoie à la destination que vous avez choisie en configurant les niveaux de journal pour les journaux du système et des applications. Le filtrage vous aide à gérer les coûts de stockage et trouver plus facilement les entrées de journal pertinentes lors du débogage.

Pour obtenir des instructions de configuration détaillées pour chaque destination, consultez les sections suivantes :

- Envoi des journaux des fonctions d'événements Lambda aux journaux CloudWatch
- Envoi des journaux des fonctions d'événements Lambda à Firehose
- Envoi des journaux des fonctions d'événements Lambda à Amazon S3

Configuration de contrôles de journalisation avancés pour les fonctions d'événement Lambda

Pour vous permettre de mieux contrôler la manière dont vos journaux de fonctions d'événements sont capturés, traités et consommés, Lambda propose les options de configuration de journalisation suivantes :

- Format de journal : choisissez entre le format texte brut et le format JSON structuré pour les journaux de votre fonction d'événement.
- Niveau du journal : pour les journaux structurés JSON, choisissez le niveau de détail des journaux auxquels Lambda envoie CloudWatch, par exemple`FATAL`,`ERROR`,, `WARN` `INFO`DEBUG, et. `TRACE`
- Groupe de journaux : choisissez le groupe de CloudWatch journaux auquel votre fonction événementielle envoie les journaux.

Pour en savoir plus sur la configuration des contrôles de journalisation avancés, consultez les sections suivantes :

- Configuration des formats de journal JSON et en texte brut
- Log-level filtrage
- Configuration des groupes de CloudWatch journaux

Configuration des formats de journal JSON et en texte brut

La capture des sorties de votre journal sous forme de paires clé-valeur JSON facilite la recherche et le filtrage lors du débogage de vos fonctions d'événement. Avec les journaux au format JSON, vous pouvez également ajouter des balises et des informations contextuelles à vos journaux. Cela peut vous aider à effectuer une analyse automatique de gros volumes de données de journal. À moins que votre flux de développement ne repose sur des outils existants qui utilisent les journaux Lambda en texte brut, nous vous recommandons de sélectionner JSON pour le format de journal.

> **Instances gérées par Lambda**
>
> Les instances gérées Lambda ne prennent en charge que le format de journal JSON. Lorsque vous créez une fonction Managed Instances, Lambda configure automatiquement le format du journal en JSON et vous ne pouvez pas le modifier en texte brut. Pour plus d'informations sur les instances gérées, consultezthe section called “Instances gérées”.

Pour tous les environnements d'exécution gérés par Lambda, vous pouvez choisir si les journaux système de votre fonction d'événement sont envoyés à CloudWatch Logs en texte brut non structuré ou au format JSON. Les journaux système sont les journaux générés par Lambda et sont parfois appelés journaux d'événements de plate-forme.

Pour les environnements d'exécution pris en charge, lorsque vous utilisez l'une des méthodes de journalisation intégrées prises en charge, Lambda peut également générer les journaux d'application de votre fonction d'événement (les journaux générés par le code de votre fonction d'événement) au format JSON structuré. Lorsque vous configurez le format de journal de votre fonction d'événement pour ces environnements d'exécution, la configuration que vous choisissez s'applique à la fois aux journaux du système et aux journaux des applications.

Pour les environnements d'exécution pris en charge, si votre fonction d'événement utilise une bibliothèque ou une méthode de journalisation prise en charge, vous n'avez pas besoin de modifier votre code existant pour que Lambda capture les journaux au format JSON structuré.

> **Note**
>
> L'utilisation du format de journal JSON ajoute des métadonnées supplémentaires et code les messages de journal sous forme d'objets JSON contenant une série de paires clé-valeur. De ce fait, la taille des messages de journal de votre fonction événementielle peut augmenter.

Temps d'exécution et méthodes de journalisation pris en charge

Lambda prend actuellement en charge la possibilité de générer des journaux d'application structurés en JSON pour les environnements d'exécution suivants.

Language	Versions prises en charge
Java	Tous les environnements d'exécution Java sauf Java 8 sur Amazon Linux 1
.NET	.NET 8 et versions ultérieures
Node.js	Node.js 16 et versions ultérieures
Python	Python 3.8 et versions ultérieures
Ruby	Ruby 4.0 et versions ultérieures

Language	Versions prises en charge
Rust	n/a

Pour que Lambda puisse envoyer les journaux d'application de votre fonction d'événement CloudWatch au format JSON structuré, votre fonction d'événement doit utiliser les outils de journalisation intégrés suivants pour générer les journaux :

- Java : L'`LambdaLogger`enregistreur ou Log4j2. Pour plus d'informations, consultez the section called "Logging".
- .NET : `ILambdaLogger` instance de l'objet de contexte. Pour plus d'informations, consultez Enregistrez et surveillez les fonctions des événements Lambda C#.
- Node.js- Les méthodes de console `console.trace`console.debug,`console.log`,`console.info`,`console.error`, et`console.warn`. Pour plus d'informations, consultez the section called "Logging".
- Python : `logging` bibliothèque Python standard. Pour plus d'informations, consultez the section called "Logging".
- Ruby : `Logger` bibliothèque Ruby standard. Pour plus d'informations, consultez the section called "Logging".
- Rust : La `tracing` caisse. Pour plus d'informations, consultez the section called "Logging".

Pour les autres environnements d'exécution Lambda gérés, Lambda ne prend actuellement en charge de manière native que la capture des journaux système au format JSON structuré. Cependant, vous pouvez toujours capturer les journaux d'applications au format JSON structuré dans n'importe quel environnement d'exécution en utilisant des outils de journalisation tels que Powertools pour générer AWS Lambda des sorties de journal au format JSON.

Formats de journal par défaut

Actuellement, le format de journal par défaut pour tous les environnements d'exécution Lambda est le texte brut. Pour les instances gérées Lambda, le format du journal est toujours JSON et ne peut pas être modifié.

Si vous utilisez déjà des bibliothèques de journalisation telles que Powertools AWS Lambda pour générer vos journaux de fonctions d'événements au format structuré JSON, vous n'avez pas besoin de modifier votre code si vous sélectionnez le format de journal JSON. Lambda n'encode pas

deux fois les journaux déjà codés au format JSON, de sorte que les journaux d'application de votre fonction d'événement continuent d'être capturés comme avant.

Format JSON pour les journaux du système

Lorsque vous configurez le format de journal de votre fonction d'événement au format JSON, chaque élément du journal système (événement de plate-forme) est capturé sous la forme d'un objet JSON contenant des paires clé-valeur avec les clés suivantes :

- `"time"` - heure à laquelle le message de journal a été généré
- `"type"` - type d'événement enregistré
- `"record"` - contenu de la sortie du journal

Le format de la valeur `"record"` varie en fonction du type d'événement enregistré. Pour plus d'informations, consultez the section called “Types d'objets d'événements de l'API de télémétrie”. Pour plus d'informations sur les niveaux de journalisation attribués aux événements du journal système, consultez the section called “Mappage des événements au niveau du journal système”.

À titre de comparaison, les deux exemples suivants montrent le même résultat de journal à la fois au format texte brut et au format JSON structuré. Notez que dans la plupart des cas, les événements du journal système contiennent plus d'informations lorsqu'ils sont produits au format JSON que lorsqu'ils sont produits en texte brut.

Example texte brut :

```
2024-03-13 18:56:24.046000 fbe8c1   INIT_START  Runtime Version:
 python:3.12.v18  Runtime Version ARN: arn:aws:lambda:eu-
west-1::runtime:edb5a058bfa782cb9cedc6d534ac8b8c193bc28e9a9879d9f5ebaaf619cd0fc0
```

Example JSON structuré :

```
{
  "time": "2024-03-13T18:56:24.046Z",
  "type": "platform.initStart",
  "record": {
    "initializationType": "on-demand",
    "phase": "init",
    "runtimeVersion": "python:3.12.v18",
    "runtimeVersionArn": "arn:aws:lambda:eu-
west-1::runtime:edb5a058bfa782cb9cedc6d534ac8b8c193bc28e9a9879d9f5ebaaf619cd0fc0"
```

```
  }
}
```

> **Note**
>
> L'API the section called “API de télémétrie” toujours des événements de plate-forme tels que `START` et `REPORT` au format JSON. La configuration du format des journaux système auxquels Lambda envoie des messages CloudWatch n'affecte pas le comportement de l'API de télémétrie Lambda.

Format JSON pour les journaux d'applications

Lorsque vous configurez le format de journal de votre fonction d'événement au format JSON, les sorties du journal d'application écrites à l'aide des bibliothèques et méthodes de journalisation prises en charge sont capturées sous forme d'objet JSON contenant des paires clé-valeur avec les clés suivantes.

- `"timestamp"` - heure à laquelle le message de journal a été généré
- `"level"` - niveau de journalisation attribué au message
- `"message"` - contenu du message de journal
- `"requestId"`(Python, .NET et Node.js) ou `"AWSrequestId"` (Java) : ID de demande unique pour l'invocation de la fonction d'événement

Selon la méthode d'exécution et de journalisation utilisée par votre fonction, cet objet JSON peut également contenir des paires de clés supplémentaires. Par exemple Node.js, si votre fonction utilise des `console` méthodes pour enregistrer les objets d'erreur à l'aide de plusieurs arguments, l'objet JSON contient des paires clé-valeur supplémentaires avec les clés `errorMessageerrorType`, et`stackTrace`. Pour en savoir plus sur les journaux au format JSON dans les différents environnements d'exécution Lambda, consultez the section called “Logging”, the section called “Logging” et the section called “Logging”.

> **Note**
>
> La clé utilisée par Lambda pour la valeur d'horodatage est différente pour les journaux système et les journaux des applications. Pour les journaux système, Lambda utilise la clé `"time"` pour maintenir la cohérence avec l'API de télémétrie. Pour les journaux

d'applications, Lambda suit les conventions des environnements d'exécution et utilise `"timestamp"`.

À titre de comparaison, les deux exemples suivants montrent le même résultat de journal à la fois au format texte brut et au format JSON structuré.

Example texte brut :

```
2024-10-27T19:17:45.586Z 79b4f56e-95b1-4643-9700-2807f4e68189 INFO some log message
```

Example JSON structuré :

```
{
    "timestamp":"2024-10-27T19:17:45.586Z",
    "level":"INFO",
    "message":"some log message",
    "requestId":"79b4f56e-95b1-4643-9700-2807f4e68189"
}
```

Configuration du format du journal de votre fonction d'événement

Pour configurer le format de journal de votre fonction d'événement, vous pouvez utiliser la console Lambda ou le AWS Command Line Interface ()AWS CLI. Vous pouvez également configurer le format de journal d'une fonction d'événement à l'aide des commandes CreateFunctionet de l'API UpdateFunctionConfigurationLambda, de la ressource AWS Serverless Application Model (AWS SAM) AWS::Serverless: :Function et de la ressource CloudFormation AWS::Lambda::Function.

La modification du format de journal de votre fonction d'événement n'affecte pas les journaux existants stockés dans CloudWatch Logs. Seuls les nouveaux journaux utilisent le format mis à jour.

Si vous modifiez le format de journal de votre fonction d'événement en JSON et que vous ne définissez pas le niveau de journal, Lambda définit automatiquement le niveau de journal d'application et le niveau de journal système de votre fonction d'événement sur INFO. Cela signifie que Lambda envoie uniquement des sorties de journal de niveau INFO ou inférieur à CloudWatch Logs. Pour en savoir plus sur le filtrage au niveau des journaux d'applications et de systèmes, consultez the section called “Log-level filtrage”

> **Note**
>
> Pour les environnements d'exécution Python, lorsque le format de journal de votre fonction d'événement est défini sur du texte brut, le paramètre de niveau de journal par défaut est WARN. Cela signifie que Lambda envoie uniquement des sorties de journal de niveau WARN ou inférieur à CloudWatch Logs. La modification du format de journal de votre fonction d'événement en JSON modifie ce comportement par défaut. Pour en savoir plus sur la journalisation dans Python, consultez the section called “Logging”.

Pour les Node.js fonctions qui émettent des journaux au format EMF (Embedded Metric Format), la modification du format de journal de votre fonction d'événement en JSON peut CloudWatch empêcher la reconnaissance de vos métriques.

> **Important**
>
> Si votre fonction d'événement utilise Powertools for AWS Lambda (TypeScript) ou les bibliothèques clientes EMF open source pour émettre des journaux EMF, mettez à jour vos bibliothèques Powertools et EMF avec les dernières versions afin de vous assurer qu'elles CloudWatch peuvent continuer à analyser correctement vos journaux. Si vous passez au format de journal JSON, nous vous recommandons également d'effectuer des tests pour garantir la compatibilité avec les métriques intégrées de votre fonction d'événement. Pour plus d’informations sur les fonctions node.js qui émettent des journaux EMF, consultez the section called “Utilisation de bibliothèques clientes au format métrique intégré (EMF) avec des journaux JSON structurés”.

Pour configurer le format de journal d'une fonction d'événement (console)

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez une fonction d'événement
3. Sur la page de configuration de la fonction d'événement, sélectionnez Outils de surveillance et d'exploitation.
4. Dans le volet de configuration de la journalisation, choisissez Modifier.
5. Sous Contenu du journal, pour Format du journal, sélectionnez Texte ou JSON.
6. Cliquez sur Enregistrer.

Pour modifier le format du journal d'une fonction existante (AWS CLI)

- Pour modifier le format de journalisation d'une fonction existante, utilisez la commande update-function-configuration. Définissez l'option `LogFormat` dans `LoggingConfig` sur `JSON` ou `Text`.

```
aws lambda update-function-configuration \
  --function-name myFunction \
  --logging-config LogFormat=JSON
```

Pour définir le format du journal lorsque vous créez une fonction (AWS CLI)

- Pour configurer le format du journal lorsque vous créez une fonction, utilisez l'option `--logging-config` de la commande create-function. Définissez `LogFormat` sur `JSON` ou `Text`. L'exemple de commande suivant crée une Node.js fonction qui génère des journaux au format JSON structuré.

  Si vous ne spécifiez pas de format de journal lorsque vous créez une fonction, Lambda utilise le format de journal par défaut pour la version d'exécution que vous sélectionnez. Pour plus d'informations sur les formats de journalisation par défaut, consultez the section called "Formats de journal par défaut".

```
aws lambda create-function \
  --function-name myFunction \
  --runtime nodejs24.x \
  --handler index.handler \
  --zip-file fileb://function.zip \
  --role arn:aws:iam::123456789012:role/LambdaRole \
  --logging-config LogFormat=JSON
```

Log-level filtrage

Lambda peut filtrer les journaux de votre fonction d'événement afin que seuls les journaux d'un certain niveau de détail ou inférieur soient envoyés aux CloudWatch journaux. Vous pouvez configurer le filtrage au niveau du journal séparément pour les journaux système de votre fonction d'événement (les journaux générés par Lambda) et les journaux d'application (les journaux générés par le code de votre fonction d'événement).

En the section called “Temps d’exécution et méthodes de journalisation pris en charge” effet, vous n'avez pas besoin de modifier le code de votre fonction d'événement pour que Lambda filtre les journaux d'application de votre fonction d'événement.

Pour tous les autres environnements d'exécution et méthodes de journalisation, le code de votre fonction d'événement doit générer les événements de journal vers `stdout` ou `stderr` sous forme d'objets au format JSON contenant une paire clé-valeur avec la clé. `"level"` Par exemple, Lambda interprète la sortie suivante vers `stdout` comme un journal de niveau DEBUG.

```
print('{"level": "debug", "msg": "my debug log", "timestamp":
 "2024-11-02T16:51:31.587199Z"}')
```

Si le champ de `"level"` valeur n'est pas valide ou est manquant, Lambda affecte à la sortie du journal le niveau INFO. Pour que Lambda utilise le champ d'horodatage, vous devez spécifier le temps dans un format d'horodatage RFC 3339 valide. Si vous ne fournissez pas d'horodatage valide, Lambda attribue au journal le niveau INFO et ajoute un horodatage pour vous.

Lorsque vous nommez la clé d’horodatage, suivez les conventions du moteur d’exécution que vous utilisez. Lambda prend en charge les conventions de dénomination les plus courantes utilisées par les environnements d'exécution gérés.

> **Note**
>
> Pour utiliser le filtrage au niveau du journal, votre fonction d'événement doit être configurée pour utiliser le format de journal JSON. Le format de journal par défaut pour tous les environnements d’exécution Lambda est actuellement le texte brut. Pour savoir comment configurer le format de journal de votre fonction d'événement au format JSON, consultezthe section called “Configuration du format du journal de votre fonction d'événement”.

Pour les journaux d’applications (les journaux générés par votre code de fonction), vous pouvez choisir entre les niveaux de journalisation suivants.

Niveau de journalisation	Utilisation standard
TRACE (le plus détaillé)	Les informations les plus précises utilisées pour tracer le chemin d’exécution de votre code

Niveau de journalisation	Utilisation standard
DEBUG	Informations détaillées pour le débogage du système
INFO	Messages qui enregistrent le fonctionnement normal de votre fonction
WARN	Messages concernant des erreurs potentiel les susceptibles d'entraîner un comportement inattendu si elles ne sont pas traitées
ERROR	Messages concernant les problèmes qui empêchent le code de fonctionner comme prévu
FATAL (moindre détail)	Messages relatifs à des erreurs graves entraînant l’arrêt du fonctionnement de l’applica tion

Lorsque vous sélectionnez un niveau de journal, Lambda envoie les journaux à ce niveau et aux niveaux inférieurs à CloudWatch Logs. Par exemple, si vous définissez le niveau de journal d'application d'une fonction d'événement sur WARN, Lambda n'envoie pas de sorties de journal aux niveaux INFO et DEBUG. Le niveau de journal d’application par défaut pour le filtrage des journaux est INFO.

Lorsque Lambda filtre les journaux d'application de votre fonction d'événement, les messages de journal sans niveau se voient attribuer le niveau de journal INFO.

Pour les journaux système (les journaux générés par le service Lambda), vous pouvez choisir entre les niveaux de journalisation suivants.

Niveau de journalisation	Usage
DEBUG (le plus détaillé)	Informations détaillées pour le débogage du système

Niveau de journalisation	Usage
INFO	Messages qui enregistrent le fonctionnement normal de votre fonction
WARN (moindre détail)	Messages concernant des erreurs potentiel les susceptibles d'entraîner un comportement inattendu si elles ne sont pas traitées

Lorsque vous sélectionnez un niveau de journal, Lambda envoie des journaux à ce niveau ou à un niveau inférieur. Par exemple, si vous définissez le niveau de journal système d'une fonction d'événement sur INFO, Lambda n'envoie pas de sorties de journal au niveau DEBUG.

Par défaut, Lambda définit le niveau de journalisation du système sur INFO. Avec ce paramètre, Lambda envoie `"start"` et `"report"` enregistre automatiquement des messages à. CloudWatch Pour recevoir des journaux système plus ou moins détaillés, définissez le niveau de journal sur DEBUG ou WARN. Pour consulter la liste des niveaux de journalisation auxquels Lambda mappe les différents événements du journal système, consultez. the section called “Mappage des événements au niveau du journal système”

Configuration du filtrage au niveau du journal

Pour configurer le filtrage au niveau du journal des applications et du système pour votre fonction d'événement, vous pouvez utiliser la console Lambda ou le (). AWS Command Line Interface AWS CLI Vous pouvez également configurer le niveau de journalisation d'une fonction d'événement à l'aide des commandes CreateFunctionet de l'API UpdateFunctionConfigurationLambda, de la ressource AWS Serverless Application Model (AWS SAM) AWS::Serverless: :Function et de la ressource CloudFormation AWS::Lambda::Function.

Notez que si vous définissez le niveau de journalisation de votre fonction d'événement dans votre code, ce paramètre a priorité sur tous les autres paramètres de journalisation que vous configurez. Par exemple, si vous utilisez la `logging` `setLevel()` méthode Python pour définir le niveau de journalisation de votre fonction d'événement sur INFO, ce paramètre a priorité sur le paramètre WARN que vous configurez à l'aide de la console Lambda.

Pour configurer le niveau de journal de l'application ou du système d'une fonction d'événement existante (console)

1. Ouvrez la page Event Functions de la console Lambda.

2. Choisissez une fonction d'événement.
3. Sur la page de configuration de la fonction d'événement, sélectionnez Outils de surveillance et d'exploitation.
4. Dans le volet de configuration de la journalisation, choisissez Modifier.
5. Sous Contenu du journal, pour le format du journal, assurez-vous que JSON est sélectionné.
6. À l'aide des boutons radio, sélectionnez le niveau de journal des applications et le niveau de journal du système souhaités pour votre fonction d'événement.
7. Cliquez sur Enregistrer.

Pour configurer le niveau de journalisation de l'application ou du système d'une fonction existante (AWS CLI)

- Pour modifier le niveau du journal de l'application ou du système d'une fonction existante, utilisez la commande update-function-configuration. Utilisez `--logging-config` pour définir `SystemLogLevel` sur l'une des valeurs suivantes : `DEBUG`, `INFO` ou `WARN`. Défini `ApplicationLogLevel` sur l'une des valeurs `DEBUG`, `INFO`, `WARN`, `ERROR` ou `FATAL`.

```
aws lambda update-function-configuration \
  --function-name myFunction \
  --logging-config LogFormat=JSON,ApplicationLogLevel=ERROR,SystemLogLevel=WARN
```

Pour configurer le filtrage au niveau du journal lorsque vous créez une fonction

- Pour configurer le filtrage au niveau du journal lorsque vous créez une fonction, utilisez l'option `--logging-config` pour définir les clés `SystemLogLevel` et `ApplicationLogLevel` de la commande create-function. A défini `SystemLogLevel` sur l'une des valeurs `DEBUG`, `INFO` ou `WARN`. Défini `ApplicationLogLevel` sur l'une des valeurs `DEBUG`, `INFO`, `WARN`, `ERROR` ou `FATAL`.

```
aws lambda create-function \
  --function-name myFunction \
  --runtime nodejs24.x \
  --handler index.handler \
  --zip-file fileb://function.zip \
  --role arn:aws:iam::123456789012:role/LambdaRole \
  --logging-config LogFormat=JSON,ApplicationLogLevel=ERROR,SystemLogLevel=WARN
```

Mappage des événements au niveau du journal système

Pour les événements de journal au niveau du système générés par Lambda, le tableau suivant définit le niveau de journal attribué à chaque événement. Pour plus d'informations sur les événements répertoriés dans le tableau, consultez the section called "Référence du schéma `Event`"

Nom de l'événement	Condition	Niveau de journalisation attribué
initStart	runtimeVersion est définie	INFO
initStart	runtimeVersion est définie	DEBUG
initialisation RuntimeDone	status=success	DEBUG
initialisation RuntimeDone	status!=success	WARN
initReport	initializationType!=on-demand	INFO
initReport	initializationType=on-demand	DEBUG
initReport	status!=success	WARN
restoreStart	runtimeVersion est définie	INFO
restoreStart	runtimeVersion n'est pas définie	DEBUG
restaurer RuntimeDone	status=success	DEBUG
restaurer RuntimeDone	status!=success	WARN
restoreReport	status=success	INFO
restoreReport	status!=success	WARN
démarrer	-	INFO
runtimeDone	status=success	DEBUG
runtimeDone	status!=success	WARN

Nom de l'événement	Condition	Niveau de journalisation attribué
report	status=success	INFO
report	status!=success	WARN
Extension	status=success	INFO
Extension	status=success	WARN
LogSubscription	-	INFO
telemetrySubscription	-	INFO
logsDropped	-	WARN

> **Note**
>
> L'API the section called "API de télémétrie" toujours l'ensemble complet des événements de la plateforme. La configuration du niveau des journaux système auxquels Lambda envoie des messages CloudWatch n'affecte pas le comportement de l'API de télémétrie Lambda.

Filtrage au niveau du journal des applications avec des environnements d'exécution personnalisés

Lorsque vous configurez le filtrage au niveau du journal des applications pour votre fonction d'événement, Lambda définit en arrière-plan le niveau du journal des applications au moment de l'exécution à l'aide de la variable d'environnement. `AWS_LAMBDA_LOG_LEVEL` Lambda définit également le format du journal de votre fonction d'événement à l'aide de la variable d'`AWS_LAMBDA_LOG_FORMAT`environnement. Vous pouvez utiliser ces variables pour intégrer les commandes de journalisation avancées de Lambda dans un environnement d'exécution personnalisé.

Pour pouvoir configurer les paramètres de journalisation d'une fonction d'événement à l'aide d'un environnement d'exécution personnalisé avec la console Lambda et les API Lambda AWS CLI, configurez votre environnement d'exécution personnalisé pour vérifier la valeur de ces variables d'environnement. Vous pouvez ensuite configurer les enregistreurs de votre environnement

d’exécution conformément au format de journal et aux niveaux de journal que vous avez sélectionnés.

Envoi des journaux des fonctions d'événements Lambda aux journaux CloudWatch

Par défaut, Lambda capture automatiquement les journaux de toutes les invocations de fonctions d'événement et les envoie à CloudWatch Logs, à condition que le rôle d'exécution de votre fonction d'événement dispose des autorisations nécessaires. Ces journaux sont, par défaut, stockés dans un groupe de journaux nommé/aws/lambda/*<function-name>*. Pour améliorer le débogage, vous pouvez insérer des instructions de journalisation personnalisées dans votre code, que Lambda intègre CloudWatch parfaitement à Logs. Si nécessaire, vous pouvez configurer votre fonction d'événement pour envoyer des journaux à un autre groupe à l'aide de la console Lambda ou de l'API AWS CLI Lambda. Pour en savoir plus, consultez the section called “Configuration des journaux CloudWatch de fonctions”.

Vous pouvez consulter les journaux des fonctions d'événements Lambda à l'aide de la console Lambda, de la CloudWatch console, du AWS Command Line Interface (AWS CLI) ou de l'API. CloudWatch Pour plus d’informations, consultez Affichage CloudWatch des journaux pour les fonctions d'événements Lambda.

> **Note**
>
> L'affichage des journaux peut prendre de 5 à 10 minutes après l'invocation d'une fonction d'événement.

Autorisations IAM requises

Votre rôle d'exécution a besoin des autorisations suivantes pour télécharger des CloudWatch journaux dans Logs :

- `logs:CreateLogGroup`
- `logs:CreateLogStream`
- `logs:PutLogEvents`

Pour en savoir plus, consultez la section Utilisation de politiques basées sur l'identité (politiques IAM) pour les CloudWatch journaux dans le guide de l'utilisateur Amazon CloudWatch .

Vous pouvez ajouter ces autorisations CloudWatch Logs à l'aide de la politique `AWSLambdaBasicExecutionRole` AWS gérée fournie par Lambda. Exécutez la commande suivante pour ajouter cette politique à votre rôle :

```
aws iam attach-role-policy --role-name your-role --policy-arn arn:aws:iam::aws:policy/
service-role/AWSLambdaBasicExecutionRole
```

Pour plus d'informations, consultez the section called "AWS politiques gérées".

Tarification

L'utilisation des journaux Lambda est gratuite ; toutefois, les frais de CloudWatch journalisation standard s'appliquent. Pour en savoir plus, consultez PricingCloudWatch (Tarification).

Configuration des groupes de CloudWatch journaux

Par défaut, crée CloudWatch automatiquement un groupe de journaux nommé `/aws/lambda/<function name>` d'après votre fonction d'événement Lambda lors de son appel initial. Pour configurer votre fonction d'événement afin d'envoyer des journaux à un groupe de journaux existant, ou pour créer un nouveau groupe de journaux pour votre fonction d'événement, vous pouvez utiliser la console Lambda ou le. AWS CLI Vous pouvez également configurer des groupes de journaux personnalisés à l'aide des commandes CreateFunctionet de l'API UpdateFunctionConfigurationLambda et de la ressource AWS Serverless Application Model (AWS SAM) AWS: :Serverless : :Function.

Vous pouvez configurer plusieurs fonctions d'événement Lambda pour envoyer des journaux au même groupe de CloudWatch journaux. Par exemple, vous pouvez utiliser un seul groupe de journaux pour stocker les journaux de toutes les fonctions d'événements Lambda qui constituent une application particulière. Lorsque vous utilisez un groupe de journaux personnalisé pour une fonction d'événement Lambda, les flux de journaux créés par Lambda incluent le nom de la fonction d'événement et la version de la fonction d'événement. Cela garantit que le mappage entre les messages du journal et les fonctions d'événement est préservé, même si vous utilisez le même groupe de journaux pour plusieurs fonctions d'événement.

Le format de dénomination des flux de journaux pour les groupes de journaux personnalisés suit cette convention :

```
YYYY/MM/DD/<function_name>[<function_version>][<execution_environment_GUID>]
```

Notez que lors de la configuration d'un groupe de journaux personnalisé, le nom que vous sélectionnez pour votre groupe de journaux doit respecter les règles de dénomination CloudWatch des journaux. En outre, les noms de groupes de journaux personnalisés ne doivent pas commencer par la chaîne `aws/`. Si vous créez un groupe de journaux personnalisé en commençant par `aws/`, Lambda ne sera pas en mesure de créer le groupe de journaux. Par conséquent, les journaux de votre fonction événementielle ne seront pas envoyés à CloudWatch.

Pour modifier le groupe de journaux d'une fonction (console)

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez une fonction d'événement.
3. Sur la page de configuration de la fonction d'événement, sélectionnez Outils de surveillance et d'exploitation.
4. Dans le volet de configuration de la journalisation, choisissez Modifier.
5. Dans le volet Groupe de journalisation, pour le groupe de CloudWatch journaux, sélectionnez Personnalisé.
6. Sous Groupe de journaux personnalisé, entrez le nom du groupe de CloudWatch journaux auquel votre fonction doit envoyer des journaux. Si vous entrez le nom d'un groupe de journaux existant, votre fonction utilisera ce groupe. S'il n'existe aucun groupe de journaux portant le nom que vous entrez, Lambda créera un nouveau groupe de journaux portant ce nom pour votre fonction.

Pour modifier le groupe de journaux d'une fonction événementielle (AWS CLI)

- Pour modifier le groupe journal d'une fonction d'événement existante, utilisez la commande update-function-configuration.

```
aws lambda update-function-configuration \
  --function-name myFunction \
  --logging-config LogGroup=myLogGroup
```

Pour spécifier un groupe de journaux personnalisé lorsque vous créez une fonction d'événement (AWS CLI)

- Pour spécifier un groupe de journaux personnalisé lorsque vous créez une nouvelle fonction d'événement Lambda à l'aide de l'option AWS CLI, utilisez l'`--logging-config`option.

L'exemple de commande suivant crée une fonction d'événement Node.js Lambda qui envoie des journaux à un groupe de journaux nommé. `myLogGroup`

```
aws lambda create-function \
  --function-name myFunction \
  --runtime nodejs24.x \
  --handler index.handler \
  --zip-file fileb://function.zip \
  --role arn:aws:iam::123456789012:role/LambdaRole \
  --logging-config LogGroup=myLogGroup
```

Autorisations du rôle d’exécution

Pour que votre fonction événementielle envoie des CloudWatch journaux à Logs, elle doit disposer de l'PutLogEventsautorisation logs :. Lorsque vous configurez le groupe de journaux de votre fonction d'événement à l'aide de la console Lambda, Lambda ajoute cette autorisation au rôle dans les conditions suivantes :

- La destination du service est définie sur CloudWatch Logs
- Le rôle d'exécution de votre fonction événementielle n'est pas autorisé à télécharger les journaux dans CloudWatch Logs (destination par défaut)

> **Note**
>
> Lambda n’ajoute aucune autorisation Put pour les destinations de journal Amazon S3 ou Firehose.

Lorsque Lambda ajoute cette autorisation, elle autorise la fonction d'événement à envoyer des journaux à n'importe quel groupe de journaux de CloudWatch journaux.

Pour empêcher Lambda de mettre automatiquement à jour le rôle d'exécution de la fonction d'événement et de le modifier manuellement, développez les autorisations et décochez Ajouter les autorisations requises.

Lorsque vous configurez le groupe de journaux de votre fonction d'événement à l'aide de AWS CLI, Lambda n'ajoute pas automatiquement l'`logs:PutLogEvents`autorisation. Ajoutez l'autorisation au

rôle d'exécution de votre fonction événementielle si elle ne l'a pas déjà. Cette autorisation est incluse dans la politique AWSLambdaBasicExecutionRolegérée.

CloudWatch journalisation pour les instances gérées Lambda

Lorsque vous utilisez des instances gérées Lambda, d'autres considérations s'appliquent à l'envoi de journaux vers CloudWatch Logs :

Exigences de mise en réseau VPC

Les instances gérées Lambda s'exécutent sur des instances EC2 appartenant au client au sein de votre VPC. Pour envoyer des CloudWatch journaux à Logs et des traces à X-Ray, vous devez vous assurer que ces AWS API sont routables depuis votre VPC. Vous avez plusieurs options:

- AWS PrivateLink (recommandé) : AWS PrivateLinkà utiliser pour créer des points de terminaison VPC pour les CloudWatch journaux et les services. X-Ray Cela permet à vos instances d'accéder à ces services en privé sans avoir besoin d'une passerelle Internet ou d'une passerelle NAT. Pour plus d'informations, consultez la section Utilisation CloudWatch des journaux avec les points de terminaison VPC de l'interface.
- Passerelle NAT : configurez une passerelle NAT pour autoriser l'accès Internet sortant à partir de vos sous-réseaux privés.
- Passerelle Internet : pour les sous-réseaux publics, assurez-vous qu'une passerelle Internet est configurée sur votre VPC.

Si CloudWatch les journaux ou les X-Ray API ne sont pas routables depuis votre VPC, les journaux et les traces de vos fonctions d'événements ne sont pas fournis.

Invocations simultanées et attribution de journaux

Les environnements d'exécution des instances gérées Lambda peuvent traiter plusieurs appels simultanément. Lorsque plusieurs appels sont exécutés simultanément, leurs entrées de journal sont entrelacées dans le même flux de journal. Pour filtrer et analyser efficacement les journaux provenant d'appels simultanés, vous devez vous assurer que chaque entrée de journal inclut l'ID de AWS demande.

Nous recommandons l'une des approches suivantes :

- Utiliser des enregistreurs d'exécution Lambda par défaut (recommandé) : Les bibliothèques de journalisation par défaut fournies par les environnements d'exécution gérés par Lambda incluent automatiquement l'ID de demande dans chaque entrée de journal.

- Implémenter une journalisation JSON structurée : si vous créez un environnement d'exécution personnalisé ou si vous avez besoin d'une journalisation personnalisée, implémentez des JSON-formatted journaux qui incluent l'ID de demande dans chaque entrée. Les instances gérées Lambda ne prennent en charge que le format de journal JSON. Incluez le `requestId` champ dans vos journaux JSON pour activer le filtrage par invocation :

```
{
  "timestamp": "2025-01-15T10:30:00.000Z",
  "level": "INFO",
  "requestId": "a1b2c3d4-e5f6-7890-abcd-ef1234567890",
  "message": "Processing request"
}
```

Grâce à l'attribution de l'ID de demande, vous pouvez filtrer CloudWatch les entrées du journal Logs pour un appel spécifique à l'aide des requêtes CloudWatch Logs Insights. Par exemple :

```
fields @timestamp, @message
| filter requestId = "a1b2c3d4-e5f6-7890-abcd-ef1234567890"
| sort @timestamp asc
```

Pour plus d'informations sur les exigences de journalisation des instances gérées Lambda, consultez. Comprendre l'environnement d'exécution des instances gérées Lambda

Affichage CloudWatch des journaux pour les fonctions d'événements Lambda

Vous pouvez consulter les CloudWatch journaux Amazon de votre fonction d'événement Lambda à l'aide de la console Lambda, de la CloudWatch console ou du (). AWS Command Line Interface AWS CLI Suivez les instructions des sections suivantes pour accéder aux journaux de votre fonction événementielle.

Diffusez les journaux des fonctions d'événements avec CloudWatch Logs Live Tail

Amazon CloudWatch Logs Live Tail vous aide à résoudre rapidement les problèmes liés à vos fonctions d'événement en affichant une liste de diffusion des nouveaux événements de journal directement dans la console Lambda. Vous pouvez consulter et filtrer les journaux ingérés à partir de vos fonctions d'événements Lambda en temps réel, ce qui vous permet de détecter et de résoudre les problèmes rapidement.

> **Note**
>
> Le coût des sessions Live Tail est calculé en fonction du temps d'utilisation de la session, par minute. Pour plus d'informations sur les tarifs, consultez Amazon CloudWatch Pricing.

Comparaison entre Live Tail et --log-type Tail

Il existe plusieurs différences entre CloudWatch Logs Live Tail et l'option LogType: Tail de l'API Lambda (`--log-type Tail`dans le AWS CLI) :

- `--log-type Tail` ne renvoie que les quatre premiers Ko des journaux d'invocation. Live Tail ne partage pas cette limite et peut recevoir jusqu'à 500 événements de journal par seconde.
- `--log-type Tail`capture et envoie les journaux avec la réponse, ce qui peut avoir un impact sur la latence de réponse de la fonction d'événement. Live Tail n'affecte pas la latence de réponse de la fonction événementielle.
- `--log-type Tail` ne prend en charge que les invocations synchrones. Live Tail fonctionne à la fois pour les invocations synchrones et asynchrones.

> **Note**
>
> Les instances gérées Lambda ne prennent pas en charge cette option. `--log-type Tail` Utilisez CloudWatch Logs Live Tail ou interrogez directement CloudWatch les journaux pour consulter les journaux des fonctions Managed Instances.

Permissions

Les autorisations suivantes sont requises pour démarrer et arrêter les sessions CloudWatch Logs Live Tail :

- `logs:DescribeLogGroups`
- `logs:StartLiveTail`
- `logs:StopLiveTail`

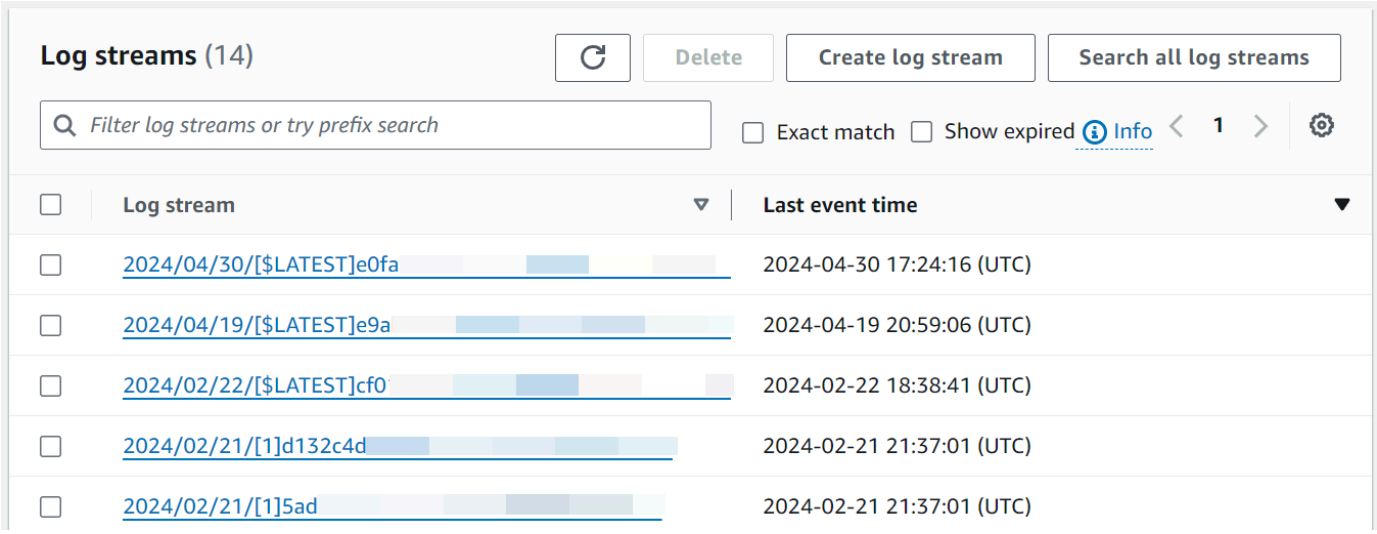
Démarrage d’une session Live Tail dans la console Lambda

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez le nom de la fonction d'événement.
3. Choisissez l’onglet Test.
4. Dans le volet Test event, sélectionnez CloudWatch Logs Live Tail.
5. Pour les groupes de journaux Select, le groupe de journaux de la fonction d'événement est sélectionné par défaut. Vous pouvez sélectionner jusqu’à cinq groupes de journaux à la fois.
6. (Facultatif) Pour m’afficher que les événements du journal contenant certains mots ou d’autres chaînes de caractères, saisissez le mot ou la chaîne dans la zone Ajouter un modèle de filtre. Le champ des filtres est sensible à la casse. Vous pouvez inclure plusieurs termes et opérateurs de motifs dans ce champ, y compris des expressions régulières (regex). Pour plus d'informations sur la syntaxe des modèles, consultez la section Syntaxe des modèles de filtres dans le guide de l'utilisateur Amazon CloudWatch Logs.
7. Sélectionnez Démarrer. Les événements du journal correspondants commencent à apparaître dans la fenêtre.
8. Pour arrêter la session Live Tail, choisissez Arrêter.

> **Note**
>
> La session Live Tail s’arrête automatiquement après 15 minutes d’inactivité ou lorsque la session de la console Lambda expire.

Accédez aux journaux des fonctions d'événements à l'aide de la console

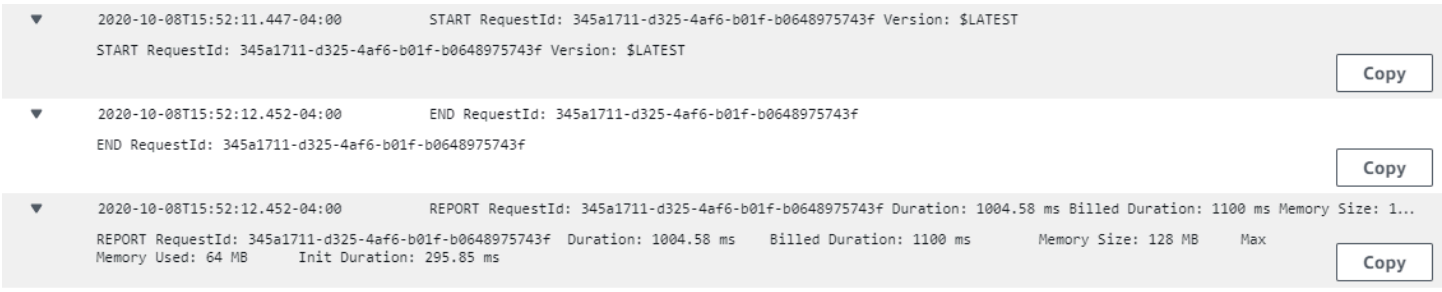
1. Ouvrez la page Event Functions de la console Lambda.
2. Sélectionnez une fonction événementielle.
3. Choisissez l’onglet Surveiller.
4. Choisissez Afficher CloudWatch les journaux pour ouvrir la CloudWatch console.
5. Faites défiler la page vers le bas et choisissez le flux de journaux pour les invocations de fonctions que vous souhaitez consulter.



Chaque instance d'une fonction d'événement Lambda possède un flux de journal dédié. Si une fonction d'événement prend de l'ampleur, chaque instance simultanée possède son propre flux de journal. Chaque fois qu'un nouvel environnement d'exécution est créé en réponse à une invocation, cela génère un nouveau flux de journaux. La convention de dénomination pour les flux de journaux est la suivante :

```
YYYY/MM/DD[Function version][Execution environment GUID]
```

Un environnement d'exécution unique écrit dans le même flux de journaux pendant sa durée de vie. Le flux de log contient les messages provenant de cet environnement d'exécution ainsi que toute sortie du code de votre fonction d'événement Lambda. Chaque message est horodaté, y compris vos journaux personnalisés. Même si votre fonction d'événement n'enregistre aucune sortie de votre code, trois instructions de journal minimales sont générées par appel (START, END et REPORT) :



Ces journaux indiquent :

- RequestId— il s'agit d'un identifiant unique généré par demande. Si la fonction d'événement Lambda tente à nouveau une demande, cet ID ne change pas et apparaît dans les journaux à chaque nouvelle tentative suivante.
- Start/End— ils marquent une seule invocation, de sorte que chaque ligne de journal entre elles appartient à la même invocation.
- Durée : durée totale d'invocation de la fonction de gestionnaire, à l'exception du code `INIT`.
- Durée facturée : applique la logique d'arrondi à des fins de facturation.
- Taille de la mémoire : quantité de mémoire allouée à la fonction d'événement.
- Mémoire maximale utilisée : quantité de mémoire maximale utilisée lors de l'invocation.
- Durée d'initialisation : temps nécessaire pour exécuter la section `INIT` de code, en dehors du gestionnaire principal.

Accédez aux journaux avec AWS CLI

AWS CLI Il s'agit d'un outil open source que vous pouvez utiliser pour interagir avec les AWS services à l'aide de commandes dans votre interface de ligne de commande. Pour effectuer les étapes de cette section, vous devez disposer de la version 2 de l'AWS CLI.

Vous pouvez utiliser AWS CLI pour récupérer les journaux d'une invocation à l'aide de l'option de commande `--log-type`. La réponse inclut un champ `LogResult` qui contient jusqu'à 4 Ko de journaux codés en base64 provenant de l'invocation.

Example récupérer un ID de journal

L'exemple suivant montre comment récupérer un ID de journal à partir du champ `LogResult` d'une fonction nommée `my-function`.

```
aws lambda invoke --function-name my-function out --log-type Tail
```

Vous devriez voir la sortie suivante:

```
{
    "StatusCode": 200,
    "LogResult":
 "U1RBUlQgUmVxdWVzdElkOiA4N2QwNDRiOC1mMTU0LTExZTgtOGNkYS0yOTc0YzVlNGZiMjEgVmVyc2lvb...",
    "ExecutedVersion": "$LATEST"
}
```

Example décoder les journaux

Dans la même invite de commandes, utilisez l'utilitaire `base64` pour décoder les journaux. L'exemple suivant montre comment récupérer les journaux encodés en base64 pour `my-function`.

```
aws lambda invoke --function-name my-function out --log-type Tail \
--query 'LogResult' --output text --cli-binary-format raw-in-base64-out | base64 --
decode
```

L'cli-binary-formatoption est obligatoire si vous utilisez AWS CLI la version 2. Pour faire de ce paramètre le paramètre par défaut, exécutez `aws configure set cli-binary-format raw-in-base64-out`. Pour plus d'informations, consultez les options de ligne de commande globales AWS CLI prises en charge dans le Guide de l'utilisateur AWS Command Line Interface version 2.

Vous devriez voir la sortie suivante :

```
START RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8 Version: $LATEST
"AWS_SESSION_TOKEN": "AgoJb3JpZ2luX2VjELj...", "_X_AMZN_TRACE_ID": "Root=1-5d02e5ca-
f5792818b6fe8368e5b51d50;Parent=191db58857df8395;Sampled=0"",ask/lib:/opt/lib",
END RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8
REPORT RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8  Duration: 79.67 ms      Billed
 Duration: 80 ms         Memory Size: 128 MB     Max Memory Used: 73 MB
```

L'utilitaire `base64` est disponible sous Linux, macOS et Ubuntu sous Windows. Les utilisateurs de macOS auront peut-être besoin d'utiliser `base64 -D`.

Example Script get-logs.sh

Dans la même invite de commandes, utilisez le script suivant pour télécharger les cinq derniers événements de journalisation. Le script utilise `sed` pour supprimer les guillemets du fichier de sortie et attend 15 secondes pour permettre la mise à disposition des journaux. La sortie comprend la réponse de Lambda, ainsi que la sortie de la commande `get-log-events`.

Copiez le contenu de l'exemple de code suivant et enregistrez-le dans votre répertoire de projet Lambda sous `get-logs.sh`.

L'cli-binary-formatoption est obligatoire si vous utilisez AWS CLI la version 2. Pour faire de ce paramètre le paramètre par défaut, exécutez `aws configure set cli-binary-format raw-in-base64-out`. Pour plus d'informations, consultez les options de ligne de commande globales AWS CLI prises en charge dans le Guide de l'utilisateur AWS Command Line Interface version 2.

```
#!/bin/bash
aws lambda invoke --function-name my-function --cli-binary-format raw-in-base64-out --
payload '{"key": "value"}' out
sed -i'' -e 's/"//g' out
sleep 15
aws logs get-log-events --log-group-name /aws/lambda/my-function --log-stream-
name stream1 --limit 5
```

Example macOS et Linux (uniquement)

Dans la même invite de commande, les utilisateurs de macOS et de Linux devront peut-être exécuter la commande suivante pour s'assurer que le script est exécutable.

```
chmod -R 755 get-logs.sh
```

Example récupérer les cinq derniers événements de journal

Dans la même invite de commande, exécutez le script suivant pour obtenir les cinq derniers événements de journalisation.

```
./get-logs.sh
```

Vous devriez voir la sortie suivante :

```
{
    "StatusCode": 200,
    "ExecutedVersion": "$LATEST"
}
{
    "events": [
        {
            "timestamp": 1559763003171,
            "message": "START RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf Version:
 $LATEST\n",
            "ingestionTime": 1559763003309
        },
        {
            "timestamp": 1559763003173,
            "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tENVIRONMENT VARIABLES\r{\r  \"AWS_LAMBDA_FUNCTION_VERSION\": \"$LATEST\",
\r ...",
            "ingestionTime": 1559763018353
```

```
        },
        {
            "timestamp": 1559763003173,
            "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tEVENT\r{\r  \"key\": \"value\"\r}\n",
            "ingestionTime": 1559763018353
        },
        {
            "timestamp": 1559763003218,
            "message": "END RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf\n",
            "ingestionTime": 1559763018353
        },
        {
            "timestamp": 1559763003218,
            "message": "REPORT RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tDuration: 26.73 ms\tBilled Duration: 27 ms \tMemory Size: 128 MB\tMax Memory Used: 75
 MB\t\n",
            "ingestionTime": 1559763018353
        }
    ],
    "nextForwardToken": "f/34783877304859518393868359594929986069206639495374241795",
    "nextBackwardToken": "b/34783877303811383369537420289090800615709599058929582080"
}
```

Analyse des journaux et journalisation structurée

Avec CloudWatch Logs Insights, vous pouvez rechercher et analyser les données des journaux à l'aide d'une syntaxe de requête spécialisée. Le service exécute des requêtes sur plusieurs groupes de journaux et fournit un filtrage puissant grâce à la correspondance de modèles glob ou d'expressions régulières.

Vous pouvez tirer parti de ces fonctionnalités en implémentant une journalisation structurée dans vos fonctions d'événements Lambda. La journalisation structurée organise vos journaux dans un format prédéfini, ce qui permet de les interroger plus facilement. L'utilisation des niveaux de journaux est une première étape importante pour générer des journaux filtrables qui séparent les messages d'information des avertissements ou des erreurs. Par exemple, considérez le Node.js code suivant :

```
exports.handler = async (event) => {
    console.log("console.log - Application is fine")
    console.info("console.info - This is the same as console.log")
    console.warn("console.warn - Application provides a warning")
    console.error("console.error - An error occurred")
```

```
}
```

Le fichier CloudWatch journal obtenu contient un champ distinct spécifiant le niveau de journalisation :

```
START RequestId: 99d91f9b-2dff-40ad-b9c8-664020094109 Version: $LATEST
2020-10-22T12:21:28.268Z        99d91f9b-2dff-40ad-b9c8-664020094109    INFO    console.log - Application is fine
2020-10-22T12:21:28.268Z        99d91f9b-2dff-40ad-b9c8-664020094109    INFO    console.info - This is the same as console.log
2020-10-22T12:21:28.268Z        99d91f9b-2dff-40ad-b9c8-664020094109    WARN    console.warn - Application provides a warning
2020-10-22T12:21:28.268Z        99d91f9b-2dff-40ad-b9c8-664020094109    ERROR   console.error - An error occurred
END RequestId: 99d91f9b-2dff-40ad-b9c8-664020094109
REPORT RequestId: 99d91f9b-2dff-40ad-b9c8-664020094109  Duration: 3.13 ms       Billed Duration: 100 ms Memory Size: 128 MB
Max Memory Used: 64 MB  Init Duration: 142.18 ms
```

Une requête CloudWatch Logs Insights peut ensuite filtrer au niveau du journal. Par exemple, pour rechercher uniquement les erreurs, vous pouvez utiliser la requête suivante :

```
fields @timestamp, @message
| filter @message like /ERROR/
| sort @timestamp desc
```

Journalisation structurée JSON

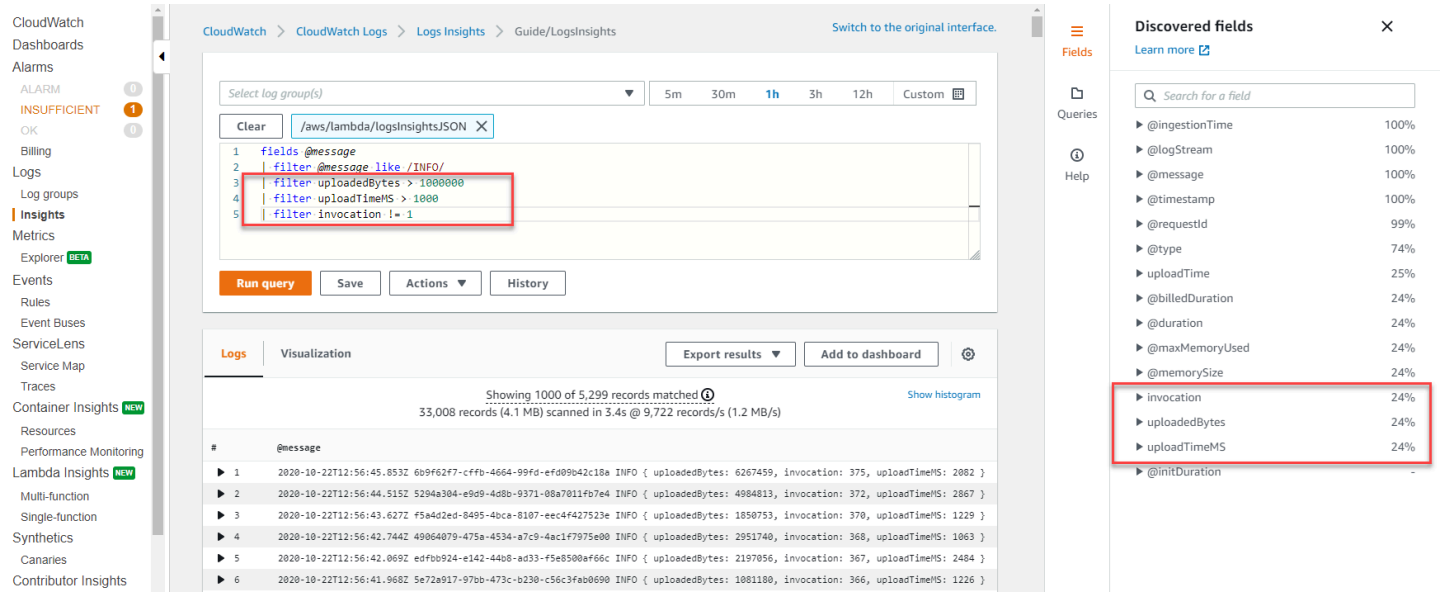
Le format JSON est couramment utilisé pour fournir une structure aux journaux d'applications. Dans l'exemple suivant, les journaux ont été convertis en JSON pour générer trois valeurs distinctes :

```
START RequestId: 22fda338-7b46-4c49-9531-efd6e8568480 Version: $LATEST
2020-10-22T11:35:59.216Z        22fda338-7b46-4c49-9531-efd6e8568480    INFO    { uploadedBytes: 5453396,
invocation: 5, uploadTimeMS: 4519 }
END RequestId: 22fda338-7b46-4c49-9531-efd6e8568480
REPORT RequestId: 22fda338-7b46-4c49-9531-efd6e8568480  Duration: 1.25 ms       Billed Duration: 100 ms Memory
Size: 128 MB    Max Memory Used: 65 MB
```

La fonctionnalité CloudWatch Logs Insights découvre automatiquement les valeurs dans la sortie JSON et analyse les messages sous forme de champs, sans avoir besoin d'une expression globale ou régulière personnalisée. À l'aide JSON-structured des journaux, la requête suivante trouve les appels pour lesquels le fichier téléchargé était supérieur à 1 Mo, le temps de téléchargement était supérieur à 1 seconde et l'invocation n'était pas un démarrage à froid :

```
fields @message
| filter @message like /INFO/
| filter uploadedBytes > 1000000
| filter uploadTimeMS > 1000
| filter invocation != 1
```

Cette requête peut produire le résultat suivant :



Les champs découverts en JSON sont automatiquement renseignés dans le menu Champs découvert à droite. Les champs standard émis par le service Lambda comportent le préfixe « @ » et vous pouvez effectuer des requêtes sur ces champs de la même manière. Les logs Lambda incluent toujours les champs @timestamp, @logStream, @message, @requestId, @duration, @billedDuration, @type, @maxMemoryUsed, @memorySize. Si cette option X-Ray est activée pour une fonction d'événement, les journaux incluent également @xray TraceId et @xraySegmentId.

Lorsqu'une source d' AWS événement telle qu'Amazon S3, Amazon SQS ou Amazon EventBridge invoque votre fonction d'événement, l'événement complet est fourni à la fonction d'événement sous forme d'entrée d'objet JSON. En enregistrant cet événement dans la première ligne de la fonction d'événement, vous pouvez ensuite effectuer une requête sur l'un des champs imbriqués à l'aide de CloudWatch Logs Insights.

Requêtes Insights utiles

Le tableau suivant présente des exemples de requêtes Insights qui peuvent être utiles pour surveiller les fonctions d'événement Lambda.

Description	Exemple de syntaxe de requête

Les 100 dernières erreurs	`fields Timestamp, LogLevel, Message`
	`| filter LogLevel == "ERR"`
	`| sort @timestamp desc`
	`| limit 100`

Description	Exemple de syntaxe de requête

Les 100 invocations les plus facturées	`filter @type = "REPORT"`
	`| fields @requestId, @billedDuration`
	`| sort by @billedDuration desc`
	`| limit 100`

Pourcentage de démarrages à froid dans le nombre total d'invocations	`filter @type = "REPORT"`
	`| stats sum(strcontains(@message,`
	` "Init Duration"))/count(*) * 100 as`
	`  coldStartPct, avg(@duration)`
	`  by bin(5m)`

Rapport de percentile sur la durée Lambda	`filter @type = "REPORT"`
	`| stats`
	`  avg(@billedDuration) as Average,`
	`  percentile(@billedDuration, 99)`
	` as NinetyNinth,`
	`  percentile(@billedDuration, 95)`
	` as NinetyFifth,`
	`  percentile(@billedDuration, 90)`
	` as Ninetieth`
	`  by bin(30m)`

Rapport de percentile sur l'utilisation de la mémoire Lambda	`filter @type="REPORT"`
	`| stats avg(@maxMemoryUsed/1024/102`
	`4) as mean_MemoryUsed,`
	`  min(@maxMemoryUsed/1024/1024) as`
	` min_MemoryUsed,`
	`  max(@maxMemoryUsed/1024/1024) as`
	` max_MemoryUsed,`
	`  percentile(@maxMemoryUsed/1`
	`024/1024, 95) as Percentile95`

Description	Exemple de syntaxe de requête

Invocations utilisant 100 % de la mémoire assignée	`filter @type = "REPORT" and @maxMemoryUsed=@memorySize`
	`| stats`
	`count_distinct(@requestId)`
	`by bin(30m)`

Mémoire moyenne utilisée lors des invocations	`avgMemoryUsedPERC,`
	`avg(@billedDuration) as avgDurationMS`
	`by bin(5m)`

Visualisation des statistiques de mémoire	`filter @type = "REPORT"`
	`| stats`
	`max(@maxMemoryUsed / 1024 / 1024) as maxMemMB,`
	`avg(@maxMemoryUsed / 1024 / 1024) as avgMemMB,`
	`min(@maxMemoryUsed / 1024 / 1024) as minMemMB,`
	`(avg(@maxMemoryUsed / 1024 / 1024) / max(@memorySize / 1024 / 1024)) * 100 as avgMemUsedPct,`
	`avg(@billedDuration) as avgDurationMS`
	`by bin(30m)`

Invocations pour lesquelles Lambda s’est fermé	`filter @message like /Process exited/` `| stats count() by bin(30m)`
Invocations dont le délai a expiré	`filter @message like /Task timed out/` `| stats count() by bin(30m)`

Description	Exemple de syntaxe de requête
Rapport de latence	`filter @type = "REPORT" | stats avg(@duration), max(@duration), min(@duration) by bin(5m)`
Over-provisioned mémoire	`filter @type = "REPORT" | stats max(@memorySize / 1024 / 1024) as provisonedMemMB, min(@maxMemoryUsed / 1024 / 1024) as smallestMemReqMB, avg(@maxMemoryUsed / 1024 / 1024) as avgMemUsedMB, max(@maxMemoryUsed / 1024 / 1024) as maxMemUsedMB, provisonedMemMB - maxMemUsedMB as overProvisionedMB`

Visualisation des journaux et tableaux de bord

Pour toute requête CloudWatch Logs Insights, vous pouvez exporter les résultats au format Markdown ou CSV. Dans certains cas, il peut être plus utile de créer des visualisations à partir de requêtes, à condition qu'il existe au moins une fonction d'agrégation. Avec cette `stats` fonction, vous pouvez définir des agrégations et des regroupements.

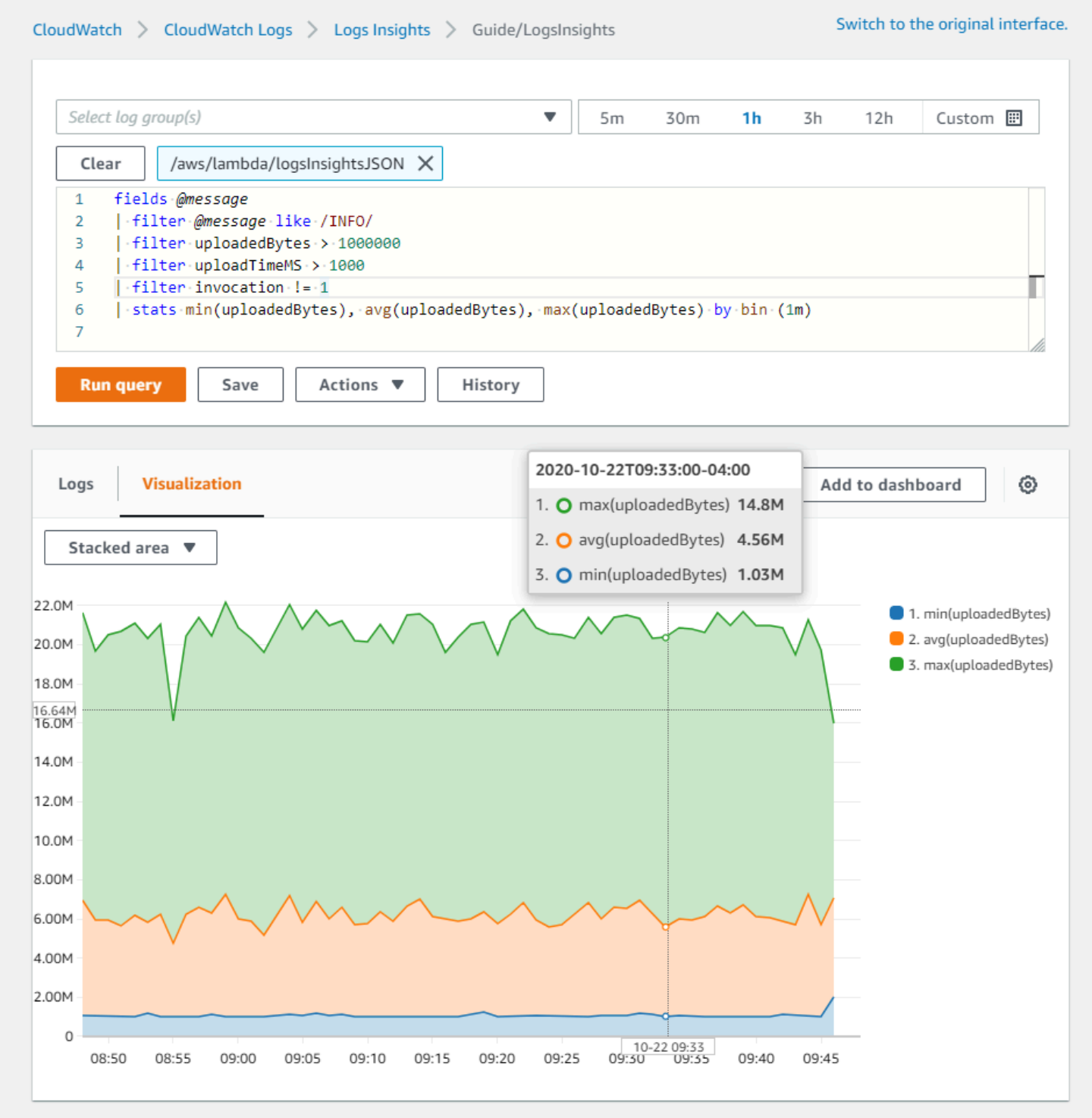
L'exemple logInsightsJSON précédent filtrait en fonction de la taille et de la durée du chargement et excluait les premières invocations. Cela générait un tableau de données. Pour surveiller un système de production, il peut être plus utile de visualiser les tailles de fichier minimales, maximales et moyennes afin de détecter les valeurs aberrantes. Pour ce faire, appliquez la fonction stats avec les agrégats requis et effectuez un regroupement en fonction d'une valeur temporelle, par exemple chaque minute :

Par exemple, réfléchissez à la requête suivante. Il s'agit du même exemple de requête que celui de la section the section called "Journalisation structurée JSON", mais avec des fonctions d'agrégation supplémentaires :

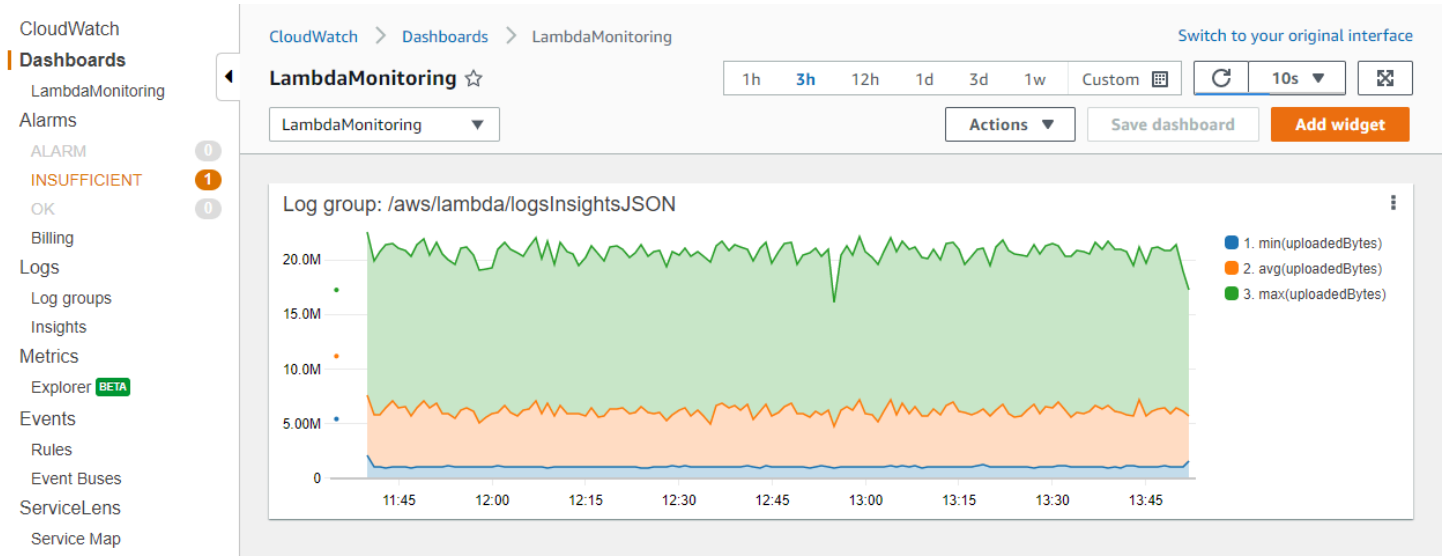
```
fields @message
```

```
| filter @message like /INFO/
| filter uploadedBytes > 1000000
| filter uploadTimeMS > 1000
| filter invocation != 1
| stats min(uploadedBytes), avg(uploadedBytes), max(uploadedBytes) by bin (1m)
```

Nous avons inclus ces agrégats car il peut être plus utile de visualiser les tailles de fichier minimale, maximale et moyenne pour identifier les valeurs aberrantes. Vous pouvez voir les résultats dans l'onglet Visualisation :



Une fois que vous avez terminé de créer la visualisation, vous pouvez éventuellement ajouter le graphique à un CloudWatch tableau de bord. Pour ce faire, choisissez Ajouter au tableau de bord au-dessus de la visualisation. Cela ajoute la requête sous forme de widget et vous pouvez sélectionner des intervalles d'actualisation automatiques, ce qui facilite le suivi continu des résultats :



Envoi des journaux des fonctions d'événements Lambda à Firehose

La console Lambda offre désormais la possibilité d'envoyer des journaux des fonctions d'événements à Firehose. Cela permet de diffuser en temps réel vos journaux vers diverses destinations prises en charge par Firehose, notamment des outils d'analytique tiers et des points de terminaison personnalisés.

> **Note**
>
> Vous pouvez configurer les journaux Lambda Event Function à envoyer à Firehose à l'aide de la console Lambda,, AWS CLI et de tous les SDK. AWS CloudFormation AWS

Tarification

Pour en savoir plus sur les tarifs, consultez CloudWatch les tarifs Amazon.

Autorisations requises pour la destination du journal Firehose

Lorsque vous utilisez la console Lambda pour configurer Firehose comme destination du journal de votre fonction d'événement, vous devez :

1. Les autorisations IAM requises pour utiliser CloudWatch Logs with Lambda.
2. Configurer des filtres d'abonnement avec Firehose. Ce filtre définit quels événements de journal sont fournis à votre flux Firehose.

Envoi des journaux des fonctions d'événements Lambda à Firehose

Dans la console Lambda, vous pouvez envoyer les journaux des fonctions d'événement directement à Firehose après avoir créé une nouvelle fonction d'événement. Pour ce faire, effectuez ces étapes :

1. Connectez-vous à la console AWS de gestion et ouvrez la console Lambda.
2. Choisissez le nom de votre fonction événementielle.
3. Cliquez sur l'onglet Configuration.
4. Choisissez l'onglet Outils de surveillance et d'exploitation.
5. Dans le volet « Configuration de la journalisation », choisissez Modifier.
6. Dans la section « Contenu du journal », sélectionnez un format de journal.
7. Dans la section « Destination du journal » procédez comme suit :
   a. Sélectionnez un service de destination.
   b. Choisissez Créer un nouveau groupe de journaux ou utilisez un Groupe de journaux existant.

      > **Note**
      >
      > Si vous choisissez un groupe de journaux existant pour une destination Firehose, assurez-vous que le groupe de journaux que vous choisissez est un type de groupe de journaux `Delivery`.

   c. Choisissez un flux Firehose.
   d. Le groupe de CloudWatch `Delivery` journaux apparaîtra.
8. Cliquez sur Enregistrer.

> **Note**
>
> Si le rôle IAM fourni dans la console ne dispose pas de l'autorisation requise, la configuration de la destination échoue. Pour résoudre ce problème, reportez-vous à Autorisations requises pour la destination du journal Firehose afin de fournir les autorisations requises.

Cross-Account Journalisation

Vous pouvez configurer Lambda pour envoyer des journaux au flux de diffusion Firehose via un autre compte. AWS Cela nécessite de définir une destination et de configurer les autorisations appropriées dans les deux comptes.

Pour obtenir des instructions détaillées sur la configuration de la journalisation entre comptes, y compris les rôles et politiques IAM requis, consultez la section Configuration d'un nouvel abonnement entre comptes dans la documentation sur les CloudWatch journaux.

Envoi des journaux des fonctions d'événements Lambda à Amazon S3

Vous pouvez configurer votre fonction d'événement Lambda pour envoyer des journaux directement à Amazon S3 à l'aide de la console Lambda. Cette fonctionnalité fournit une solution rentable pour le stockage des journaux à long terme et permet d'utiliser de puissantes options d'analyse à l'aide de services comme Athena.

> **Note**
>
> Vous pouvez configurer les journaux Lambda Event Function à envoyer à Amazon S3 à l'aide de la console Lambda, AWS CLI AWS CloudFormation, et de tous les SDK. AWS

Tarification

Pour en savoir plus sur les tarifs, consultez CloudWatch les tarifs Amazon.

Autorisations requises pour la destination du journal Amazon S3

Lorsque vous utilisez la console Lambda pour configurer Amazon S3 comme destination du journal de votre fonction d'événement, vous devez :

1. Les autorisations IAM requises pour utiliser CloudWatch Logs with Lambda.
2. Pour Configurer un filtre d'abonnements aux CloudWatch journaux pour envoyer les journaux des fonctions d'événements Lambda à Amazon S3. Ce filtre définit quels événements de journal sont fournis à votre compartiment Amazon S3.

Configurer un filtre d'abonnements aux CloudWatch journaux pour envoyer les journaux des fonctions d'événements Lambda à Amazon S3

Pour envoyer des CloudWatch journaux depuis Logs vers Amazon S3, vous devez créer un filtre d'abonnement. Ce filtre définit quels événements de journal sont fournis à votre compartiment Amazon S3. Le groupe de journaux doit se trouver dans la même région que votre compartiment Amazon S3.

Pour créer un filtre d'abonnements pour Amazon S3

1. Créez un compartiment Amazon Simple Storage Service (Amazon S3). Nous vous recommandons d'utiliser un bucket créé spécifiquement pour CloudWatch Logs. Toutefois, si vous souhaitez utiliser un compartiment existant, passez directement à l'étape 2.

   Exécutez la commande suivante en remplaçant l'espace réservé à la région par la région que vous voulez utiliser :

   ```
   aws s3api create-bucket --bucket amzn-s3-demo-bucket2 --create-bucket-configuration
    LocationConstraint=region
   ```

   > **Note**
   >
   > `amzn-s3-demo-bucket2` est un exemple de nom de compartiment Amazon S3. Il est réservé. Pour que cette procédure fonctionne, vous devez le remplacer par le nom unique de votre compartiment Amazon S3.

   Voici un exemple de sortie :

   ```
   {
       "Location": "/amzn-s3-demo-bucket2"
   }
   ```

2. Créez le rôle IAM qui autorise CloudWatch Logs à placer des données dans votre compartiment Amazon S3. Cette politique inclut une clé contextuelle aws : SourceArn global condition pour éviter le problème de sécurité confus lié aux adjoints. Pour plus d'informations consultez Prévention du problème de l'adjoint confus.

   a. Utilisez un éditeur de texte pour créer une politique d'approbation dans un fichier `~/TrustPolicyForCWL.json` comme suit :

```
{
    "Statement": {
        "Effect": "Allow",
        "Principal": { "Service": "logs.amazonaws.com" },
        "Condition": {
            "StringLike": {
                "aws:SourceArn": "arn:aws:logs:region:123456789012:*"
            }
         },
        "Action": "sts:AssumeRole"
    }
}
```

b. Utilisez la commande create-role pour créer le rôle IAM, en spécifiant le fichier de politique d'approbation. Notez la Role.Arn valeur renvoyée, car vous en aurez besoin ultérieurement :

```
aws iam create-role \
 --role-name CWLtoS3Role \
 --assume-role-policy-document file://~/TrustPolicyForCWL.json
{
    "Role": {
        "AssumeRolePolicyDocument": {
            "Statement": {
                "Action": "sts:AssumeRole",
                "Effect": "Allow",
                "Principal": {
                    "Service": "logs.amazonaws.com"
                },
                "Condition": {
                    "StringLike": {
                        "aws:SourceArn": "arn:aws:logs:region:123456789012:*"
                    }
                }
            }
        },
        "RoleId": "AAOIIAH450GAB4HC5F431",
        "CreateDate": "2015-05-29T13:46:29.431Z",
        "RoleName": "CWLtoS3Role",
        "Path": "/",
        "Arn": "arn:aws:iam::123456789012:role/CWLtoS3Role"
    }
}
```

3. Créez une politique d'autorisation pour définir les actions que CloudWatch Logs peut effectuer sur votre compte. D'abord, utilisez un éditeur de texte pour créer une stratégie d'autorisations dans un fichier `~/PermissionsForCWL.json` :

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["s3:PutObject"],
      "Resource": ["arn:aws:s3:::amzn-s3-demo-bucket2/*"]
    }
  ]
}
```

   Associez la politique d'autorisations au rôle à la commande `put-role-policy` suivante :

```
aws iam put-role-policy --role-name CWLtoS3Role --policy-name Permissions-Policy-For-
S3 --policy-document file://~/PermissionsForCWL.json
```

4. Créez un groupe de journaux `Delivery` ou utilisez un groupe de journaux `Delivery` existant.

```
aws logs create-log-group --log-group-name my-logs --log-group-class DELIVERY --
region REGION_NAME
```

5. `PutSubscriptionFilter` pour configurer la destination

```
aws logs put-subscription-filter
--log-group-name my-logs
--filter-name my-lambda-delivery
--filter-pattern ""
--destination-arn arn:aws:s3:::amzn-s3-demo-bucket2
--role-arn arn:aws:iam::123456789012:role/CWLtoS3Role
--region REGION_NAME
```

Envoi des journaux des fonctions d'événements Lambda à Amazon S3

Dans la console Lambda, vous pouvez envoyer les journaux des fonctions d'événement directement à Amazon S3 après avoir créé une nouvelle fonction d'événement. Pour ce faire, effectuez ces étapes :

1. Connectez-vous à la console AWS de gestion et ouvrez la console Lambda.
2. Choisissez le nom de votre fonction événementielle.
3. Cliquez sur l'onglet Configuration.
4. Choisissez l'onglet Outils de surveillance et d'exploitation.
5. Dans le volet « Configuration de la journalisation », choisissez Modifier.
6. Dans la section « Contenu du journal », sélectionnez un format de journal.
7. Dans la section « Destination du journal » procédez comme suit :
   a. Sélectionnez un service de destination.
   b. Choisissez Créer un nouveau groupe de journaux ou utilisez un Groupe de journaux existant.

   > **Note**
   >
   > Si vous choisissez un groupe de journaux existant pour une destination Amazon S3, assurez-vous que le groupe de journaux que vous choisissez est un type de groupe de journaux `Delivery`.

   c. Choisissez un compartiment Amazon S3 comme destination pour vos journaux de fonctions d'événements.
   d. Le groupe de CloudWatch `Delivery` journaux apparaît.
8. Cliquez sur Enregistrer.

> **Note**
>
> Si le rôle IAM fourni dans la console ne dispose pas des autorisations requises, la configuration de la destination échoue. Pour résoudre ce problème, reportez-vous à la section Autorisations requises pour la destination du journal Amazon S3.

Cross-Account Journalisation

Vous pouvez configurer Lambda pour envoyer des journaux vers un compartiment Amazon S3 dans un autre AWS compte. Cela nécessite de définir une destination et de configurer les autorisations appropriées dans les deux comptes.

Pour obtenir des instructions détaillées sur la configuration de la journalisation entre comptes, y compris les rôles et politiques IAM requis, consultez la section Configuration d'un nouvel abonnement entre comptes dans la documentation sur les CloudWatch journaux.

Logging AWS Lambda Appels d'API utilisant AWS CloudTrail

AWS Lambda est intégré à AWS CloudTrailun service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un Service AWS. CloudTrail capture les appels d'API pour Lambda sous forme d'événements. Les appels capturés incluent des appels de la console Lambda et les appels de code vers les opérations d'API Lambda. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite à Lambda, l'adresse IP à partir de laquelle la demande a été faite, la date à laquelle elle a été faite et des informations supplémentaires.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer :

- Si la demande a été effectuée avec des informations d'identification d'utilisateur root ou d'utilisateur root.
- Si la demande a été faite au nom d'un utilisateur du centre d'identité IAM.
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la requête a été effectuée par un autre Service AWS.

CloudTrail est actif dans votre compte Compte AWS lorsque vous créez le compte et vous avez automatiquement accès à l'historique des CloudTrail événements. L'historique des CloudTrail événements fournit un enregistrement consultable, consultable, téléchargeable et immuable des 90 derniers jours des événements de gestion enregistrés dans un. Région AWS Pour plus d'informations, consultez la section Utilisation de l'historique des CloudTrail événements dans le guide de AWS CloudTrail l'utilisateur. La consultation de CloudTrail l'historique des événements est gratuite.

Pour un enregistrement continu des événements de vos 90 Compte AWS derniers jours, créez un magasin de données sur les événements de Trail ou CloudTrailLake.

CloudTrail sentiers

Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Tous les sentiers créés à l'aide du Console de gestion AWS sont multirégionaux. Vous ne pouvez créer un journal de suivi en une ou plusieurs régions à l'aide de l' AWS CLI. Il est recommandé de créer un parcours multirégional, car vous capturez l'activité dans l'ensemble Régions AWS de votre compte. Si vous créez un journal de suivi pour une seule région, il convient de n'afficher

que les événements enregistrés dans le journal de suivi pour une seule région Région AWS. Pour plus d'informations sur les journaux de suivi, consultez Créez un journal de suivi dans vos Compte AWS et Création d'un journal de suivi pour une organisation dans le AWS CloudTrail Guide de l'utilisateur.

Vous pouvez envoyer une copie de vos événements de gestion en cours dans votre compartiment Amazon S3 gratuitement CloudTrail en créant un journal. Toutefois, des frais de stockage Amazon S3 sont facturés. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification. Pour obtenir des informations sur la tarification Amazon S3, consultez Tarification Amazon S3.

CloudTrail Stockages de données sur les événements du lac

CloudTrail Lake vous permet de lancer SQL-based des requêtes sur vos événements. CloudTrail Lake convertit les événements existants au format JSON basé sur les lignes au format Apache ORC. ORC est un format de stockage en colonnes qui est optimisé pour une récupération rapide des données. Les événements sont agrégés dans des magasins de données d'événement. Ceux-ci constituent des collections immuables d'événements basées sur des critères que vous sélectionnez en appliquant des sélecteurs d'événements avancés. Les sélecteurs que vous appliquez à un magasin de données d'événement contrôlent les événements qui persistent et que vous pouvez interroger. Pour plus d'informations sur CloudTrail Lake, consultez la section Travailler avec AWS CloudTrail Lake dans le guide de AWS CloudTrail l'utilisateur.

CloudTrail Les stockages et requêtes de données sur les événements de Lake entraînent des coûts. Lorsque vous créez un magasin de données d'événement, vous choisissez l'option de tarification que vous voulez utiliser pour le magasin de données d'événement. L'option de tarification détermine le coût d'ingestion et de stockage des événements, ainsi que les périodes de conservation par défaut et maximale pour le magasin de données d'événement. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification.

Événements relatifs aux données Lambda dans CloudTrail

Les événements de données fournissent des informations sur les opérations de ressources effectuées sur ou dans une ressource (par exemple, lecture ou écriture de données dans un objet Amazon S3). Ils sont également connus sous le nom opérations de plans de données. Les événements de données sont souvent des activités à fort volume. Par défaut, CloudTrail n'enregistre pas la plupart des événements liés aux données et l'historique des CloudTrail événements ne les enregistre pas.

Un événement de CloudTrail données enregistré par défaut pour les services pris en charge est`LambdaESMDisabled`. Pour en savoir plus sur l'utilisation de cet événement afin de résoudre les problèmes liés aux mappages des sources d'événements Lambda, consultez the section called "Utilisation CloudTrail pour résoudre les problèmes liés aux sources d'événements Lambda désactivées".

Des frais supplémentaires s'appliquent pour les événements de données. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification.

Vous pouvez enregistrer les événements de données pour le type de `AWS::Lambda::Function` ressource à l'aide de la CloudTrail console ou AWS CLI des opérations de CloudTrail l'API. Pour plus d'informations sur la façon de journaliser les événements de données, consultez Journalisation des événements de données avec la Console de gestion AWS et Journalisation des événements de données avec l' AWS Command Line Interface dans le Guide de l'utilisateur AWS CloudTrail .

Le tableau suivant répertorie les types de ressources Lambda pour lesquels vous pouvez journaliser les événements de données. La colonne Type d'événement de données (console) indique la valeur à choisir dans la liste des types d'événements de données de la CloudTrail console. La colonne de valeur resources.type indique la **`resources.type`** valeur que vous devez spécifier lors de la configuration de sélecteurs d'événements avancés à l'aide des API or. AWS CLI CloudTrail La CloudTrail colonne Data APIs logged to indique les appels d'API enregistrés CloudTrail pour le type de ressource.

Type d'événement de données (console)	valeur resources.type	API de données connectées à CloudTrail
Lambda	`AWS::Lambda::Function`	Invoke

Vous pouvez configurer des sélecteurs d'événements avancés pour filtrer les champs `eventName`, `readOnly` et `resources.ARN` afin de ne journaliser que les événements importants pour vous. L'exemple suivant est la vue JSON d'une configuration d'événements de données qui enregistre les événements pour une fonction d'événement spécifique uniquement. Pour plus d'informations sur ces champs, consultez AdvancedFieldSelector dans la Référence des API AWS CloudTrail .

```
[
  {
    "name": "function-invokes",
```

```
    "fieldSelectors": [
      {
        "field": "eventCategory",
        "equals": [
          "Data"
        ]
      },
      {
        "field": "resources.type",
        "equals": [
          "AWS::Lambda::Function"
        ]
      },
      {
        "field": "resources.ARN",
        "equals": [
          "arn:aws:lambda:us-east-1:111122223333:function:hello-world"
        ]
      }
    ]
  }
]
```

Événements de gestion Lambda dans CloudTrail

Les événements de gestion fournissent des informations sur les opérations de gestion effectuées sur les ressources de votre Compte AWS. Ils sont également connus sous le nom opérations de plan de contrôle. Par défaut, CloudTrail enregistre les événements de gestion.

Lambda prend en charge la journalisation des actions suivantes sous forme d'événements de gestion dans des fichiers CloudTrail journaux.

> **Note**
>
> Dans le fichier CloudTrail journal, ils `eventName` peuvent inclure des informations de date et de version, mais cela fait toujours référence à la même action d'API publique. Par exemple, l'action `GetFunction` apparaît sous la forme de `GetFunction20150331v2`. La liste suivante indique les cas où le nom de l'événement diffère du nom de l'action d'API.

- AddLayerVersionPermission

- AddPermission(nom de l'événement :`AddPermission20150331v2`)
- CreateAlias(nom de l'événement :`CreateAlias20150331`)
- CreateEventSourceMapping(nom de l'événement :`CreateEventSourceMapping20150331`)
- CreateFunction(nom de l'événement :`CreateFunction20150331`)

  (Les paramètres `Environment` et `ZipFile` ne figurent pas dans les journaux CloudTrail pour `CreateFunction`.)
- CreateFunctionUrlConfig
- DeleteAlias(nom de l'événement :`DeleteAlias20150331`)
- DeleteCodeSigningConfig
- DeleteEventSourceMapping(nom de l'événement :`DeleteEventSourceMapping20150331`)
- DeleteFunction(nom de l'événement :`DeleteFunction20150331`)
- DeleteFunctionConcurrency(nom de l'événement :`DeleteFunctionConcurrency20171031`)
- DeleteFunctionUrlConfig
- DeleteProvisionedConcurrencyConfig
- GetAlias(nom de l'événement :`GetAlias20150331`)
- GetEventSourceMapping
- GetFunction
- GetFunctionUrlConfig
- GetFunctionConfiguration
- GetLayerVersionPolicy
- GetPolicy
- ListEventSourceMappings
- ListFunctions
- ListFunctionUrlConfigs
- PublishLayerVersion(nom de l'événement :`PublishLayerVersion20181031`)

  (Le `ZipFile` paramètre est omis dans les CloudTrail journaux de`PublishLayerVersion`.)
- PublishVersion(nom de l'événement :`PublishVersion20150331`)
- PutFunctionConcurrency(nom de l'événement :`PutFunctionConcurrency20171031`)
- PutFunctionCodeSigningConfig

- PutFunctionEventInvokeConfig
- PutProvisionedConcurrencyConfig
- PutRuntimeManagementConfig
- RemovePermission(nom de l'événement :`RemovePermission20150331v2`)
- TagResource(nom de l'événement :`TagResource20170331v2`)
- UntagResource(nom de l'événement :`UntagResource20170331v2`)
- UpdateAlias(nom de l'événement :`UpdateAlias20150331`)
- UpdateCodeSigningConfig
- UpdateEventSourceMapping(nom de l'événement :`UpdateEventSourceMapping20150331`)
- UpdateFunctionCode(nom de l'événement :`UpdateFunctionCode20150331v2`)

  (Le `ZipFile` paramètre est omis dans les CloudTrail journaux de`UpdateFunctionCode`.)
- UpdateFunctionConfiguration(nom de l'événement :`UpdateFunctionConfiguration20150331v2`)

  (Le `Environment` paramètre est omis dans les CloudTrail journaux de`UpdateFunctionConfiguration`.)
- UpdateFunctionEventInvokeConfig
- UpdateFunctionUrlConfig

Utilisation CloudTrail pour résoudre les problèmes liés aux sources d'événements Lambda désactivées

Lorsque vous modifiez l'état du mappage d'une source d'événement à l'aide de l'action d'UpdateEventSourceMappingAPI, l'appel d'API est enregistré en tant qu'événement de gestion CloudTrail. Les mappages de sources d'événements peuvent également passer directement à l'état `Disabled` en raison d'erreurs.

Pour les services suivants, Lambda publie l'événement de `LambdaESMDisabled` données CloudTrail lorsque votre source d'événements passe à l'état Désactivé :

- Amazon Simple Queue Service (Amazon SQS)
- Amazon DynamoDB
- Amazon Kinesis

Lambda ne prend en charge cet événement pour aucun autre type de mappage des sources d'événements.

Pour recevoir des alertes lorsque les mappages de sources d'événements pour les services pris en charge passent à l'`Disabled`état, configurez une alarme dans Amazon à CloudWatch l'aide de l'`LambdaESMDisabled` CloudTrail événement. Pour en savoir plus sur la configuration d'une CloudWatch alarme, voir Création d' CloudWatch alarmes pour CloudTrail des événements : exemples.

L'entité `serviceEventDetails` figurant dans le message d'événement `LambdaESMDisabled` contient l'un des codes d'erreur suivants.

`RESOURCE_NOT_FOUND`

La ressource spécifiée dans la demande n'existe pas.

`FUNCTION_NOT_FOUND`

La fonction d'événement attachée à la source d'événement n'existe pas.

`REGION_NAME_NOT_VALID`

Le nom de région fourni à la source d'événement ou à la fonction d'événement n'est pas valide.

`AUTHORIZATION_ERROR`

Les autorisations n'ont pas été définies ou sont mal configurées.

`FUNCTION_IN_FAILED_STATE`

Le code de la fonction d'événement ne se compile pas, a rencontré une exception irrécupérable ou un mauvais déploiement s'est produit.

Exemples d'événements Lambda

Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'opération d'API demandée, la date et l'heure de l'opération, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics. Les événements n'apparaissent donc pas dans un ordre spécifique.

L'exemple suivant montre les entrées du CloudTrail journal pour les `DeleteFunction` actions `GetFunction` et.

> **Note**
>
> `eventName` peut inclure des informations de date et de version, comme `"GetFunction20150331"`, mais il s'agit toujours de la même API publique.


```
{
  "Records": [
    {
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/myUserName",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "myUserName"
      },
      "eventTime": "2015-03-18T19:03:36Z",
      "eventSource": "lambda.amazonaws.com",
      "eventName": "GetFunction",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "127.0.0.1",
      "userAgent": "Python-httplib2/0.8 (gzip)",
      "errorCode": "AccessDenied",
      "errorMessage": "User: arn:aws:iam::111122223333:user/myUserName is not
 authorized to perform: lambda:GetFunction on resource: arn:aws:lambda:us-
west-2:111122223333:function:other-acct-function",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "7aebcd0f-cda1-11e4-aaa2-e356da31e4ff",
      "eventID": "e92a3e85-8ecd-4d23-8074-843aabfe89bf",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    },
    {
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/myUserName",
        "accountId": "111122223333",
```

```
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "myUserName"
      },
      "eventTime": "2015-03-18T19:04:42Z",
      "eventSource": "lambda.amazonaws.com",
      "eventName": "DeleteFunction20150331",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "127.0.0.1",
      "userAgent": "Python-httplib2/0.8 (gzip)",
      "requestParameters": {
        "functionName": "basic-node-task"
      },
      "responseElements": null,
      "requestID": "a2198ecc-cda1-11e4-aaa2-e356da31e4ff",
      "eventID": "20b84ce5-730f-482e-b2b2-e8fcc87ceb22",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    }
  ]
}
```


Pour plus d'informations sur le contenu des CloudTrail enregistrements, voir le contenu des CloudTrail enregistrements dans le Guide de AWS CloudTrail l'utilisateur.

Visualisez les invocations de la fonction d'événement Lambda à l'aide de AWS X-Ray

Vous pouvez l'utiliser AWS X-Ray pour visualiser les composants de votre application, identifier les goulots d'étranglement liés aux performances et résoudre les demandes ayant entraîné une erreur. Vos fonctions d'événement Lambda envoient des données de suivi et X-Ray X-Ray les traitent pour générer une carte des services et des résumés de suivi consultables.

Lambda prend en charge deux modes de suivi pour X-Ray : `Active` et. `PassThrough` Grâce au `Active` suivi, Lambda crée automatiquement des segments de trace pour les invocations de fonctions d'événement et les envoie à. X-Ray `PassThroughl`e mode, quant à lui, propage simplement le contexte de suivi aux services en aval.

Si vous avez activé le `Active` suivi pour votre fonction d'événement, Lambda envoie automatiquement des traces à X-Ray des requêtes échantillonnées. Généralement, un service en amont, tel qu'Amazon API Gateway ou une application hébergée sur Amazon EC2 équipée du X-Ray SDK, décide si les demandes entrantes doivent être suivies, puis ajoute cette décision d'échantillonnage en tant qu'en-tête de suivi. Lambda utilise cet en-tête pour décider d’envoyer des traces ou non. Les traces provenant des producteurs de messages en amont, tels qu'Amazon SQS, sont automatiquement liées aux traces des fonctions d'événement Lambda en aval, créant ainsi une vue de bout en bout de l'application dans son intégralité. Pour plus d’informations, consultez Traçage des applications événementielles dans le Guide du développeur AWS X-Ray .

> **Note**
>
> X-Ray le suivi n'est actuellement pas pris en charge pour les fonctions d'événement Lambda avec Amazon Managed Streaming for Apache Kafka (Amazon MSK), Apache Kafka autogéré, Amazon MQ avec ActiveMQ et RabbitMQ, ou les mappages de sources d'événements Amazon DocumentDB.

Pour activer le suivi actif de votre fonction d'événement Lambda à l'aide de la console, procédez comme suit :

Pour activer le traçage actif

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez une fonction d'événement.

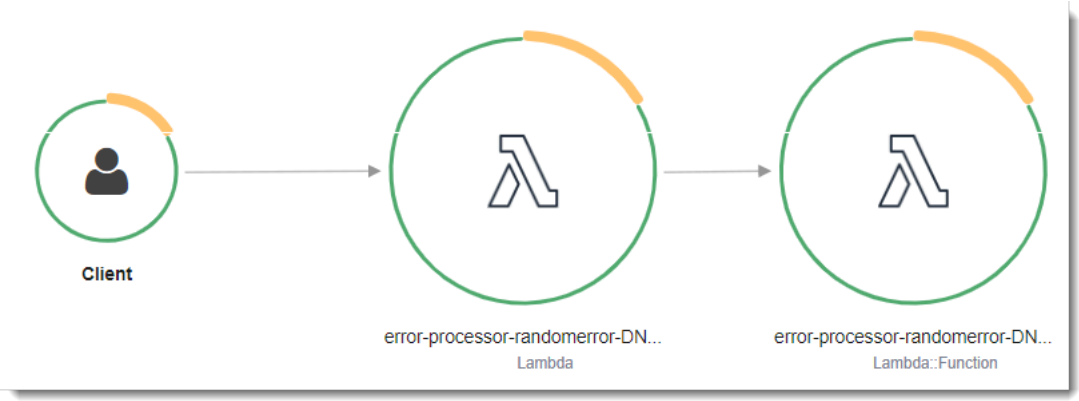
3. Choisissez Configuration, puis choisissez Outils de surveillance et d'opérations.
4. Dans Outils de surveillance supplémentaires, choisissez Modifier.
5. Sous Signaux CloudWatch d'application et AWS X-Ray sélectionnez Activer les traces de service Lambda.
6. Cliquez sur Enregistrer.

Votre fonction événementielle a besoin d'une autorisation pour télécharger des données de suivi sur X-Ray. Lorsque vous activez le suivi dans la console Lambda, Lambda ajoute les autorisations requises au rôle d'exécution de votre fonction d'événement. Dans le cas contraire, ajoutez la AWSXRayDaemonWriteAccesspolitique au rôle d'exécution.

X-Ray ne retrace pas toutes les demandes jusqu'à votre application. X-Ray applique un algorithme d'échantillonnage pour garantir l'efficacité du suivi, tout en fournissant un échantillon représentatif de toutes les demandes. Le taux d'échantillonnage est 1 demande par seconde et 5 % de demandes supplémentaires. Vous ne pouvez pas configurer le taux X-Ray d'échantillonnage pour vos fonctions.

Comprendre les X-Ray traces

Dans X-Ray, un suivi enregistre des informations relatives à une demande traitée par un ou plusieurs services. Lambda enregistre deux segments par suivi, ce qui a pour effet de créer deux nœuds sur le graphique du service. L'image suivante met en évidence ces deux nœuds :



Le premier nœud sur la gauche représente le service Lambda qui reçoit la demande d'invocation. Le deuxième nœud représente votre fonction d'événement Lambda spécifique.

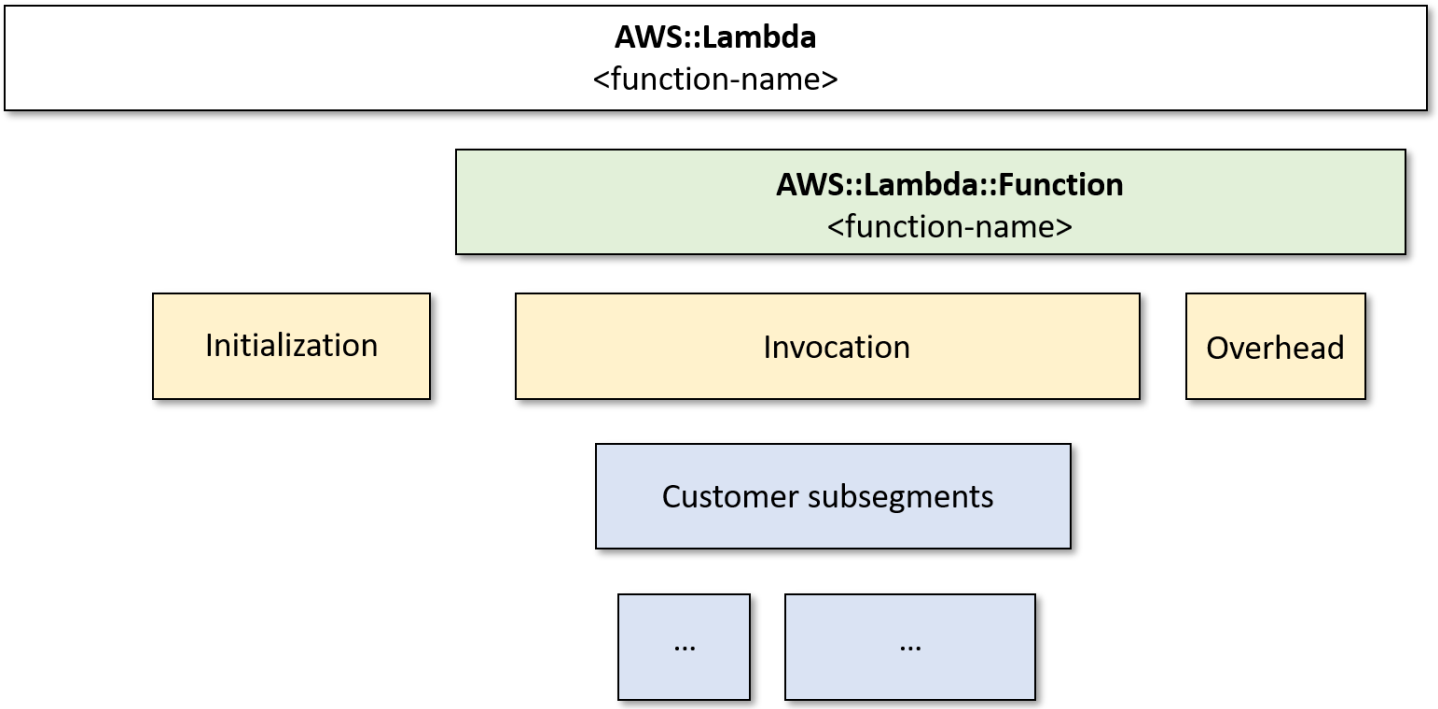
Le segment enregistré pour le service Lambda, `AWS::Lambda`, couvre toutes les étapes nécessaires à la préparation de l'environnement d'exécution Lambda. Cela inclut la planification de la MicroVM, la création ou le déblocage d'un environnement d'exécution avec les ressources que vous avez configurées, ainsi que le téléchargement de votre code de la fonction et de toutes les couches.

Le `AWS::Lambda::Function` segment est destiné au travail effectué par la fonction d'événement.

> **Note**
>
> AWS met actuellement en œuvre des modifications du service Lambda. En raison de ces modifications, vous pouvez constater des différences mineures entre la structure et le contenu des messages du journal système et des segments de trace émis par les différentes fonctions d'événement Lambda de votre ordinateur. Compte AWS
> Cette modification affecte les sous-segments du segment de fonction. Les paragraphes suivants décrivent les anciens et les nouveaux formats de ces sous-segments.
> Ces modifications seront mises en œuvre au cours des prochaines semaines, et toutes les fonctions, Régions AWS sauf en Chine et dans les GovCloud régions, seront transférées pour utiliser le nouveau format des messages de journal et des segments de trace.

Old-style AWS X-Ray Structure du segment Lambda

L'ancienne X-Ray structure du `AWS::Lambda` segment se présente comme suit :



Dans ce format, le segment de fonction comporte des sous-segments pour `Initialization`, `Invocation` et `Overhead`. Pour SnapStart uniquement, il existe également un sous-segment `Restore` (non représenté sur ce schéma).

Le sous-segment `Initialization` représente la phase d'initialisation du cycle de vie de l'environnement d'exécution Lambda. Au cours de cette phase, Lambda initialise les extensions, initialise l'environnement d'exécution, et exécute le code d'initialisation de la fonction.

Le sous-segment `Invocation` représente la phase d'invocation où Lambda invoque le gestionnaire de fonction. Cela commence par l'enregistrement de l'exécution et de l'extension et se termine lorsque l'exécution est prête à envoyer la réponse.

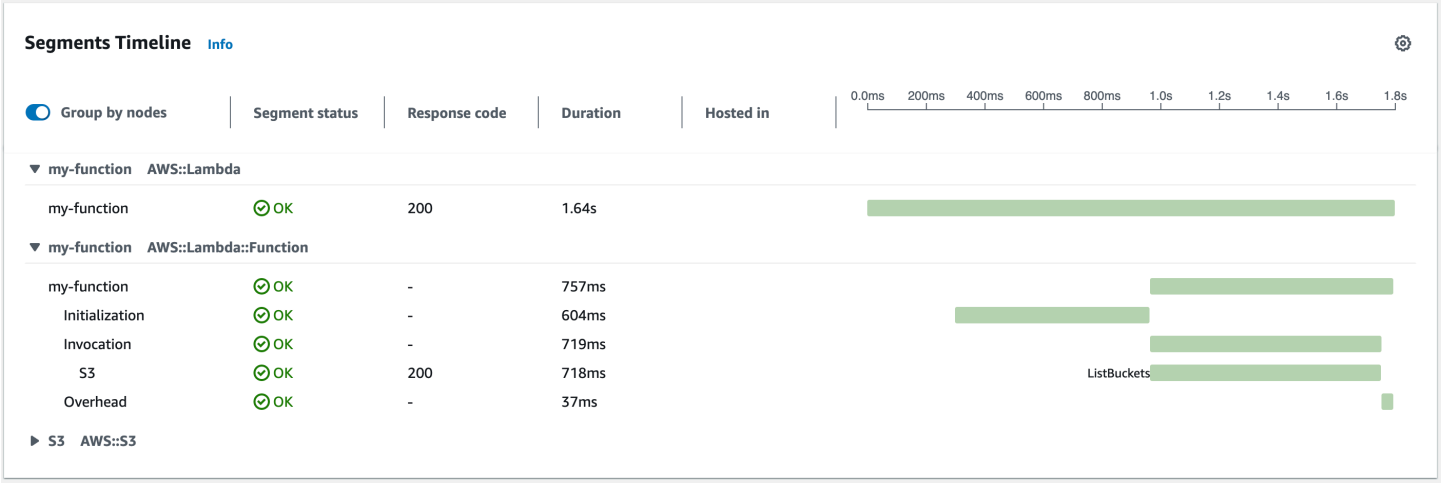
(Lambda SnapStart uniquement) Le `Restore` sous-segment indique le temps nécessaire à Lambda pour restaurer un instantané, charger le moteur d'exécution et exécuter les éventuels hooks d'exécution après la restauration. Le processus de restauration des instantanés peut inclure du temps consacré à des activités en dehors de la MicroVM. Cette heure est indiquée dans le sous-segment `Restore`. Le temps passé en dehors de la microVM pour restaurer un instantané ne vous est pas facturé.

Le sous-segment `Overhead` représente la phase qui se produit entre le moment où l'exécution envoie la réponse et le signal pour l'invocation suivante. Pendant ce temps, l'exécution termine toutes les tâches liées à une invocation et se prépare à geler l'environnement de test (sandbox).

> **Important**
>
> Vous pouvez utiliser le X-Ray SDK pour étendre le `Invocation` sous-segment avec des sous-segments supplémentaires pour les appels en aval, les annotations et les métadonnées. Vous ne pouvez pas accéder directement au segment de fonction ou enregistrer une tâche effectuée en dehors de la portée d'invocation du gestionnaire.

Pour plus d'informations sur les phases de l'environnement d'exécution Lambda, consultez the section called "Environnement d'exécution".

Un exemple de trace utilisant l'ancienne X-Ray structure est illustré dans le schéma suivant.

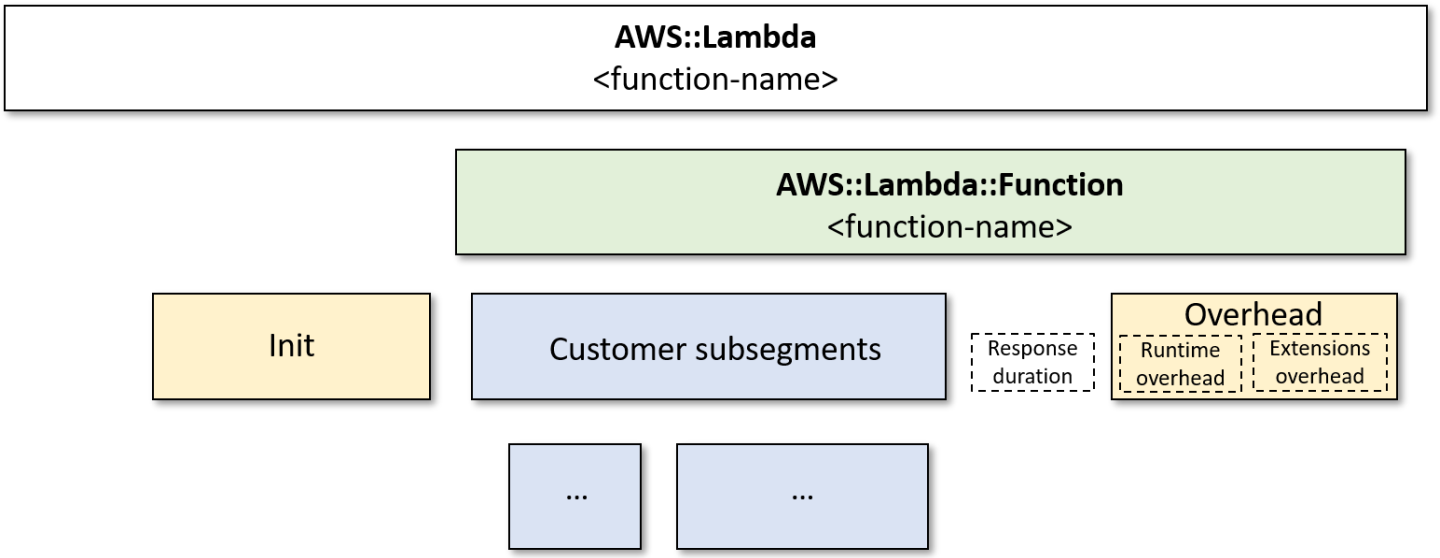


Notez les deux segments de l'exemple. Les deux sont nommés my-function, mais l'un a pour origine `AWS::Lambda` et l'autre a pour origine `AWS::Lambda::Function`. Si le segment `AWS::Lambda` affiche une erreur, cela signifie que le service Lambda a rencontré un problème. Si le `AWS::Lambda::Function` segment affiche une erreur, cela signifie que votre fonction d'événement a rencontré un problème.

> **Note**
>
> Parfois, vous remarquerez peut-être un écart important entre les phases d'initialisation et d'invocation de la fonction dans vos X-Ray traces. Pour les fonctions utilisant la simultanéité provisionnée, cela est dû au fait que Lambda initialise vos instances de fonction bien avant l'invocation. Pour les fonctions événementielles utilisant une simultanéité non réservée (à la demande), Lambda peut initialiser de manière proactive une instance de fonction, même en l'absence d'invocation. Visuellement, ces deux cas se manifestent par un écart de temps entre les phases d'initialisation et d'invocation.

New-style AWS X-Ray Structure du segment Lambda

Le nouveau style de X-Ray structure du `AWS::Lambda` segment se présente comme suit :

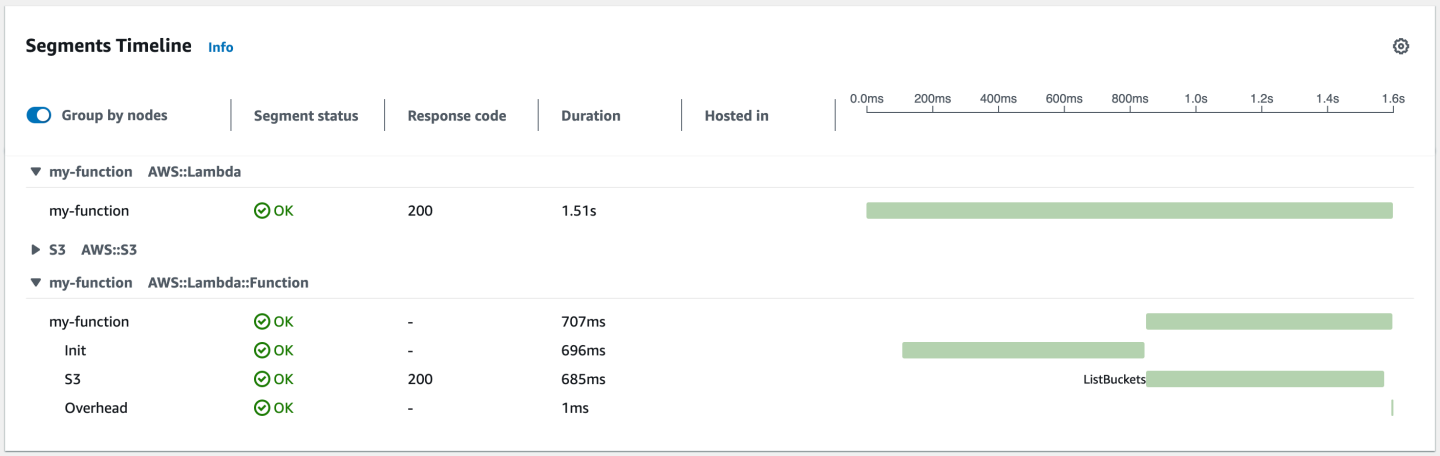


Dans ce nouveau format, le sous-segment `Init` représente la phase d'initialisation du cycle de vie de l'environnement d'exécution Lambda comme auparavant.

Le nouveau format ne contient pas de segment d'invocation. À la place, les sous-segments du client sont directement rattachés au segment `AWS::Lambda::Function`. Ce segment contient les métriques suivantes sous forme d'annotations :

- `aws.responseLatency` : le temps nécessaire à l'exécution de la fonction
- `aws.responseDuration` : le temps nécessaire pour transmettre la réponse au client
- `aws.runtimeOverhead` : le temps supplémentaire dont l'exécution a eu besoin pour se terminer
- `aws.extensionOverhead` : le temps supplémentaire dont les extensions ont eu besoin pour se terminer

Un exemple de trace utilisant la X-Ray structure du nouveau style est illustré dans le schéma suivant.



Notez les deux segments de l'exemple. Les deux sont nommés my-function, mais l'un a pour origine `AWS::Lambda` et l'autre a pour origine `AWS::Lambda::Function`. Si le segment `AWS::Lambda` affiche une erreur, cela signifie que le service Lambda a rencontré un problème. Si le `AWS::Lambda::Function` segment affiche une erreur, cela signifie que votre fonction d'événement a rencontré un problème.

Consultez les rubriques suivantes pour une présentation du suivi dans Lambda spécifique de chaque langage :

- Instrumentation du Node.js code dans AWS Lambda
- Instrumentation du code Python dans AWS Lambda
- Instrumentation du code Ruby dans AWS Lambda
- Instrumentation du code Java dans AWS Lambda
- Instrumentation du code Go AWS Lambda
- Instrumentation du code C# dans AWS Lambda

Pour obtenir la liste complète des services qui prennent en charge l'instrumentation active, consultez Services AWS pris en charge dans le Guide du développeur AWS X-Ray .

Comportement de suivi par défaut dans Lambda

Si le suivi `Active` n'est pas activé, Lambda passe en mode de suivi `PassThrough` par défaut.

En `PassThrough` mode, Lambda transmet l'en-tête de X-Ray suivi aux services en aval, mais n'envoie pas de traces automatiquement. Cela est vrai même si l'en-tête de suivi contient la décision d'échantillonner la demande. Si le service en amont ne fournit pas d'en-tête de X-Ray suivi, Lambda génère un en-tête et prend la décision de ne pas échantillonner. Cependant, vous pouvez envoyer vos propres traces en appelant des bibliothèques de suivi à partir de votre code Event Function.

> **Note**
>
> Auparavant, Lambda envoyait automatiquement des traces lorsque des services en amont, comme Amazon API Gateway, ajoutaient un en-tête de suivi. En n'envoyant pas de traces automatiquement, Lambda vous permet de contrôler les fonctions d'événement qui sont importantes pour vous. Si votre solution repose sur ce comportement de suivi passif, passez au suivi `Active`.

Autorisations du rôle d’exécution

Lambda a besoin des autorisations suivantes pour envoyer des données de suivi à. X-Ray Ajoutez-les au rôle d'exécution de votre fonction événementielle.

- radiographie : PutTraceSegments
- radiographie : PutTelemetryRecords

Ces autorisations sont incluses dans la politique AWSXRayDaemonWriteAccessgérée.

Activation du suivi **`actif`** avec l'API Lambda

Pour gérer la configuration du suivi avec le AWS SDK AWS CLI ou le SDK, utilisez les opérations d'API suivantes :

- UpdateFunctionConfiguration
- GetFunctionConfiguration
- CreateFunction

L'exemple de AWS CLI commande suivant active le suivi actif sur une fonction nommée my-function.

```
aws lambda update-function-configuration --function-name my-function \
--tracing-config Mode=Active
```

Le mode de suivi fait partie de la configuration spécifique de la version lorsque vous publiez une version de votre fonction. Vous ne pouvez pas modifier le mode de suivi sur une version publiée.

Activation du suivi **`actif`** avec CloudFormation

Pour activer le suivi d'une `AWS::Lambda::Function` ressource dans un CloudFormation modèle, utilisez la `TracingConfig` propriété.

Example fonction-inline.yml — Configuration du suivi

```
Resources:
  function:
    Type: AWS::Lambda::Function
    Properties:
      TracingConfig:
```

```
        Mode: Active
      ...
```

Pour une `AWS::Serverless::Function` ressource AWS Serverless Application Model (AWS SAM), utilisez la `Tracing` propriété.

Example template.yml — Configuration du suivi

```
Resources:
  function:
    Type: AWS::Serverless::Function
    Properties:
      Tracing: Active
      ...
```

Surveillez les performances des fonctions événementielles avec Amazon CloudWatch Lambda Insights

Amazon CloudWatch Lambda Insights collecte et agrège les indicateurs de performance d'exécution et les journaux de performance de la fonction d'événement Lambda pour vos applications sans serveur. Cette page explique comment activer et utiliser Lambda Insights pour diagnostiquer les problèmes liés à vos fonctions d'événement Lambda.

Sections

- Comment Lambda Insights surveille les applications sans serveur
- Tarification
- Environnements d'exécution pris en charge
- Activation de Lambda Insights dans la console Lambda
- Activation de Lambda Insights par programme
- Utilisation du tableau de bord Lambda Insights
- Exemple de flux de travail pour détecter les anomalies de la fonction événementielle
- Exemple de flux de travail utilisant des requêtes pour résoudre les problèmes liés à une fonction événementielle
- Quelle est la prochaine étape ?

Comment Lambda Insights surveille les applications sans serveur

CloudWatch Lambda Insights est une solution de surveillance et de dépannage pour les applications sans serveur exécutées sur. AWS Lambda La solution collecte, agrège et résume les métriques de niveau système, notamment l'utilisation de temps d'UC, de mémoire, de disque et de réseau. Il collecte, agrège et résume également les informations de diagnostic telles que les démarrages à froid et les arrêts des opérateurs Lambda pour vous aider à isoler les problèmes liés à vos fonctions d'événement Lambda et à les résoudre rapidement.

Lambda Insights utilise une nouvelle extension CloudWatch Lambda Insights, fournie sous forme de couche Lambda. Lorsque vous activez cette extension sur une fonction d'événement Lambda pour un environnement d'exécution pris en charge, elle collecte des métriques au niveau du système et émet un seul événement de journal des performances pour chaque appel de cette fonction d'événement Lambda. CloudWatch utilise le formatage des métriques intégré pour extraire les métriques des

événements du journal. Pour plus d'informations, consultez la section Utilisation des AWS Lambda extensions.

La couche Lambda Insights étend `CreateLogStream` et `PutLogEvents` pour le groupe de journaux `/aws/lambda-insights/`.

Tarification

Lorsque vous activez Lambda Insights pour votre fonction d'événement Lambda, Lambda Insights rapporte 8 mesures par fonction d'événement et chaque appel de fonction d'événement envoie environ 1 Ko de données de journal à. CloudWatch Vous ne payez que pour les statistiques et les journaux signalés pour votre fonction d'événement par Lambda Insights. Aucun frais minimum ni aucune politique d'utilisation obligatoire des services ne sont appliqués. Vous ne payez pas pour Lambda Insights si la fonction d'événement n'est pas invoquée. Pour un exemple de tarification, consultez les CloudWatch tarifs Amazon.

Environnements d'exécution pris en charge

Vous pouvez utiliser Lambda Insights avec n'importe quel runtime prenant en charge les extensions Lambda.

Activation de Lambda Insights dans la console Lambda

Vous pouvez activer la surveillance améliorée de Lambda Insights sur les fonctions d'événement Lambda nouvelles et existantes. Lorsque vous activez Lambda Insights sur une fonction d'événement dans la console Lambda pour un environnement d'exécution pris en charge, Lambda ajoute l'extension Lambda Insights en tant que couche à votre fonction d'événement et vérifie ou tente d'associer la politique au rôle d'exécution de votre fonction d'événement. CloudWatchLambdaInsightsExecutionRolePolicy

Pour activer Lambda Insights dans la console Lambda

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez la fonction de votre événement.
3. Cliquez sur l’onglet Configuration.
4. Dans le menu de gauche, sélectionnez Outils de surveillance et d’exploitation.
5. Dans le volet Outils de surveillance supplémentaires, choisissez Modifier.
6. Sous CloudWatch Lambda Insights, activez Enhanced monitoring (Surveillance améliorée).

7. Choisissez Enregistrer.

Activation de Lambda Insights par programme

Vous pouvez également activer Lambda Insights à l'aide de la CLI AWS Command Line Interface AWS Serverless Application Model (AWS CLI), (SAM) ou du. CloudFormation Cloud Development Kit AWS (AWS CDK)Lorsque vous activez Lambda Insights par programmation sur une fonction d'événement pour un environnement d'exécution pris en charge, associez la CloudWatchLambdaInsightsExecutionRolePolicypolitique CloudWatch au rôle d'exécution de votre fonction d'événement.

Pour plus d'informations, consultez Getting started with Lambda Insights dans le guide de CloudWatch l'utilisateur Amazon.

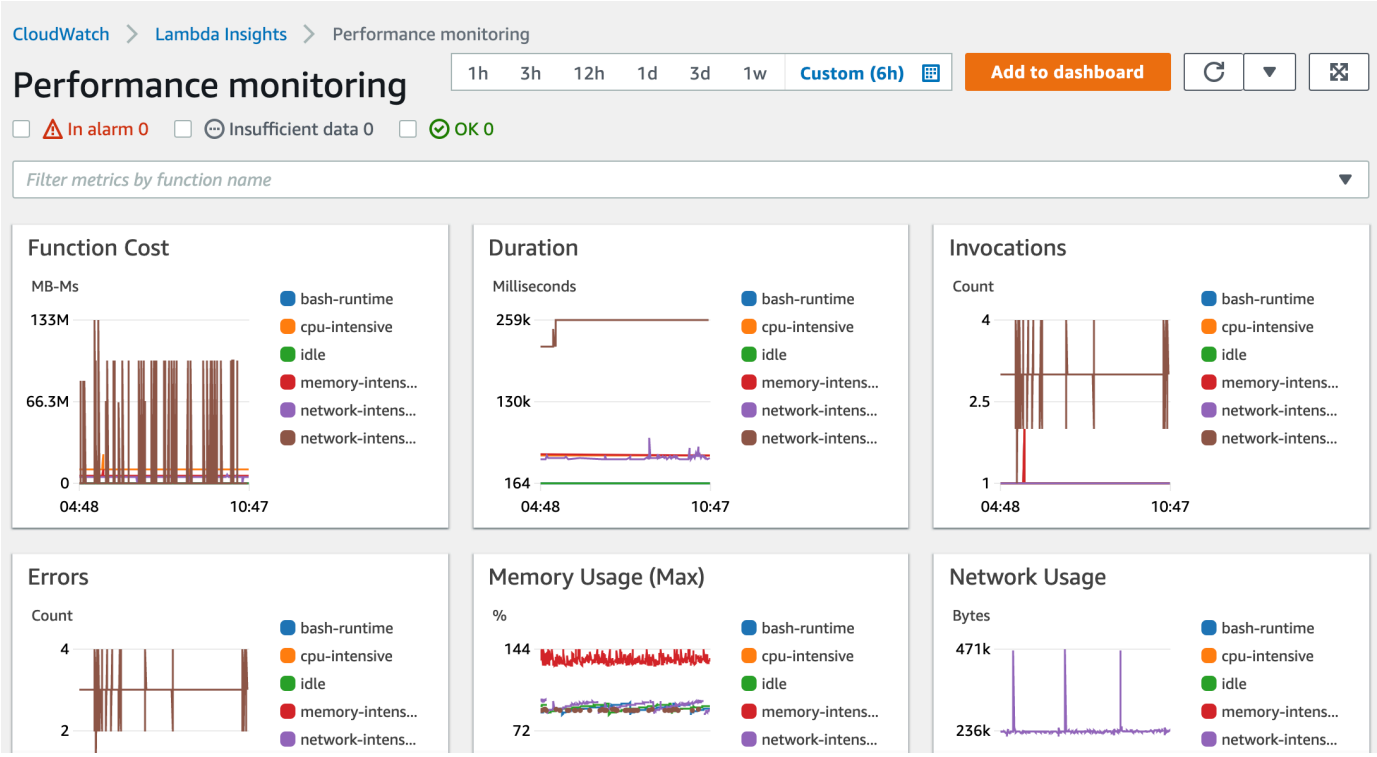
Utilisation du tableau de bord Lambda Insights

Le tableau de bord Lambda Insights comporte deux vues dans la CloudWatch console : la vue d'ensemble multifonction et la vue monofonctionnelle. La vue d'ensemble multifonction regroupe les métriques d'exécution des fonctions d'événement Lambda dans le compte courant AWS et la région. La vue à fonction unique affiche les métriques d'exécution disponibles pour une seule fonction d'événement Lambda.

Vous pouvez utiliser la vue d'ensemble multifonctions du tableau de bord Lambda Insights dans la CloudWatch console pour identifier les fonctions d'événement Lambda surutilisées ou sous-utilisées. Vous pouvez utiliser la vue à fonction unique du tableau de bord Lambda Insights dans la CloudWatch console pour résoudre les demandes individuelles.

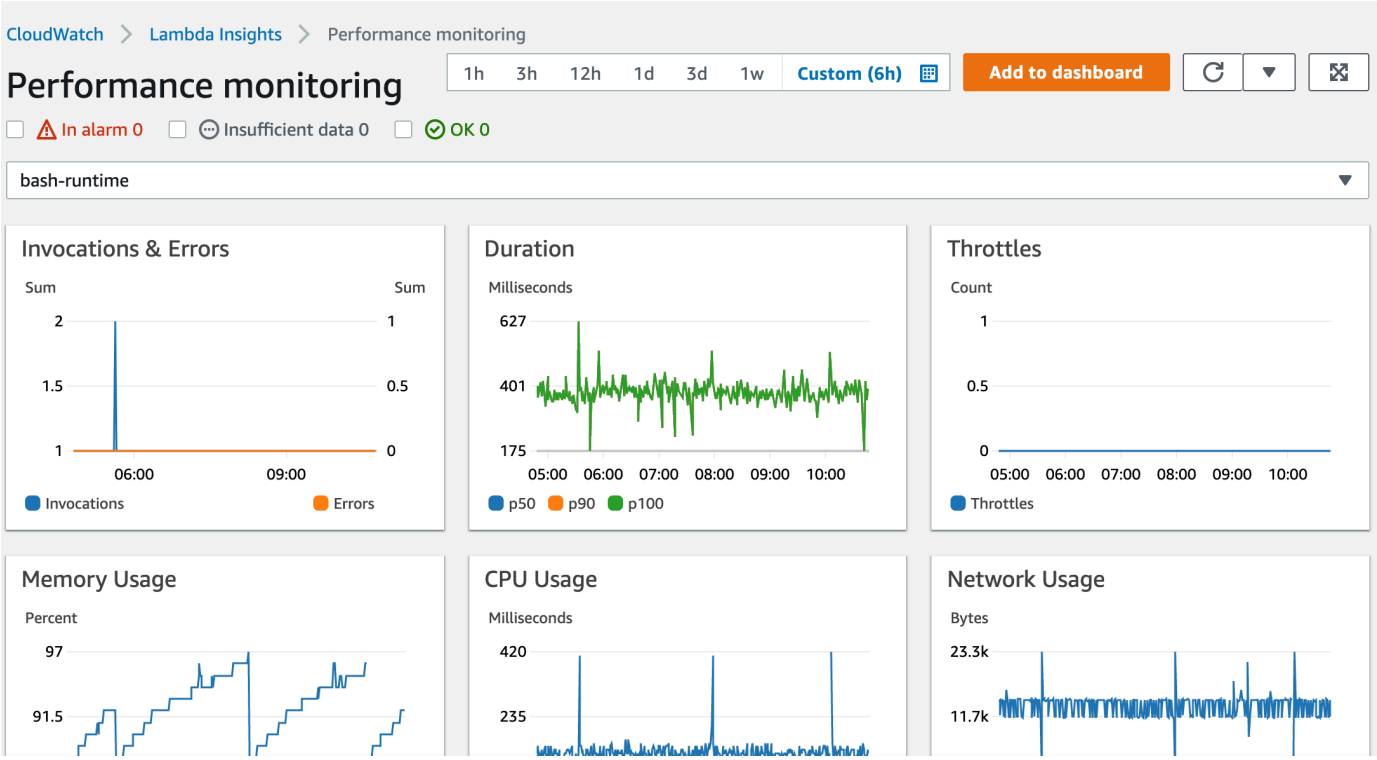
Pour afficher les métriques d'exécution de toutes les fonctions événementielles

1. Ouvrez la Multi-functionpage dans la CloudWatch console.
2. Choisissez parmi les plages de temps prédéfinies ou choisissez une plage de temps personnalisée.
3. (Facultatif) Choisissez Ajouter au tableau de bord pour ajouter les widgets à votre CloudWatch tableau de bord.



Pour afficher les métriques d'exécution d'une seule fonction d'événement

1. Ouvrez la Single-functionpage dans la CloudWatch console.
2. Choisissez parmi les plages de temps prédéfinies ou choisissez une plage de temps personnalisée.
3. (Facultatif) Choisissez Ajouter au tableau de bord pour ajouter les widgets à votre CloudWatch tableau de bord.



Pour plus d'informations, consultez la section Création et utilisation de widgets sur les CloudWatch tableaux de bord.

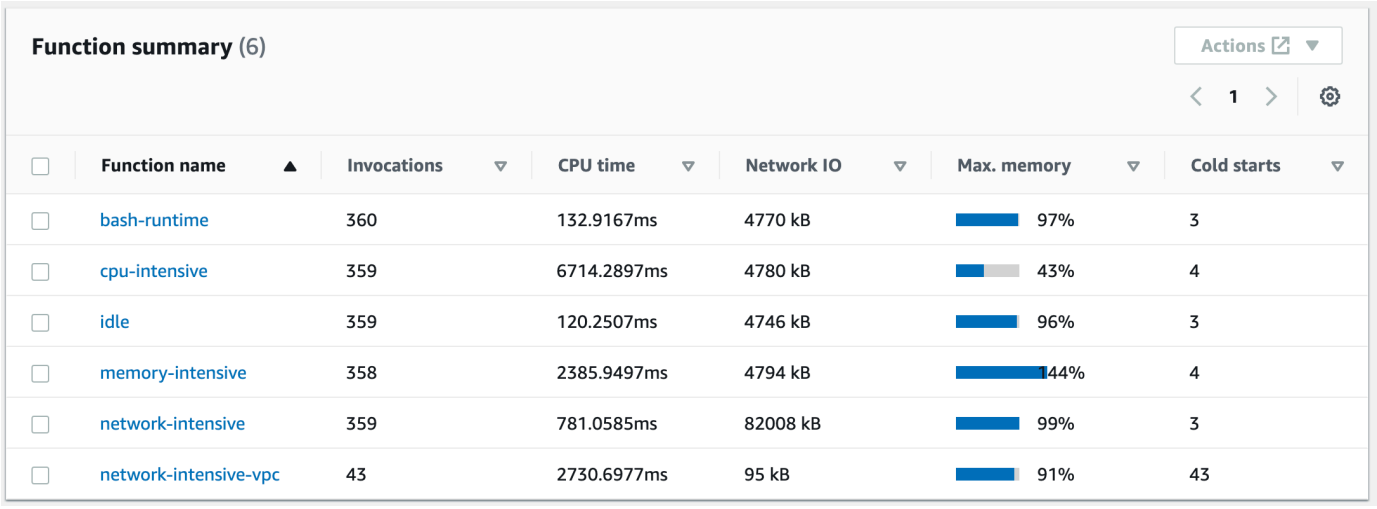
Exemple de flux de travail pour détecter les anomalies de la fonction événementielle

Vous pouvez utiliser la vue d'ensemble multifonctions du tableau de bord Lambda Insights pour identifier et détecter les anomalies de mémoire de calcul associées à votre fonction d'événement. Par exemple, si la vue d'ensemble des fonctions multifonctions indique qu'une fonction événementielle utilise une grande quantité de mémoire, vous pouvez consulter les mesures détaillées d'utilisation de la mémoire dans le volet Utilisation de la mémoire. Vous pouvez ensuite accéder au tableau de bord des métriques pour activer la détection d'anomalies ou créer une alarme.

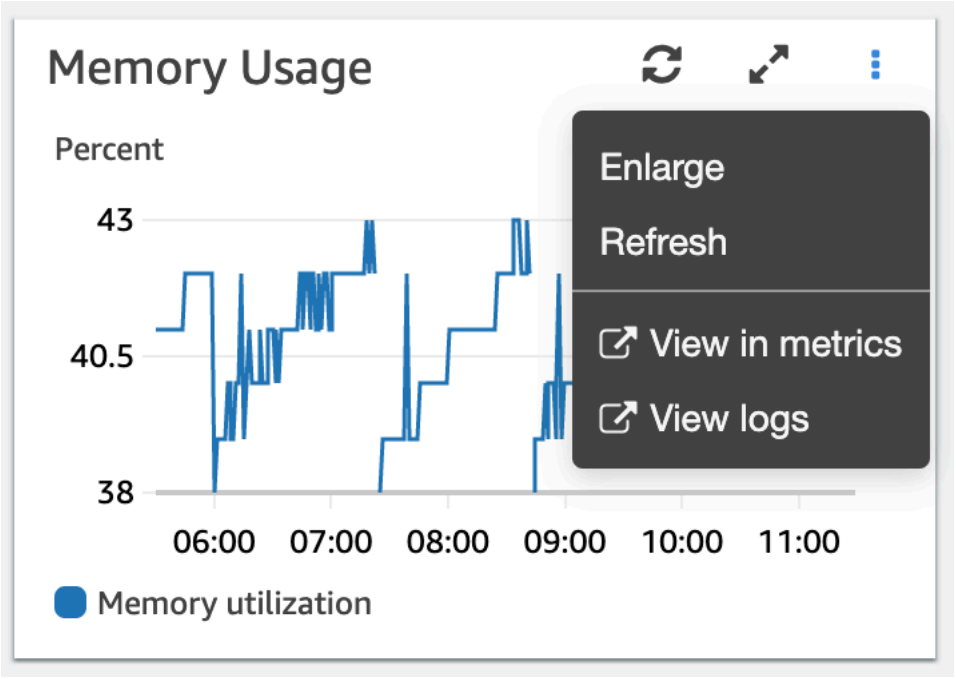
Pour activer la détection des anomalies pour une fonction événementielle

1. Ouvrez la Multi-functionpage dans la CloudWatch console.
2. Sous Résumé des fonctions, choisissez le nom de votre fonction événementielle.

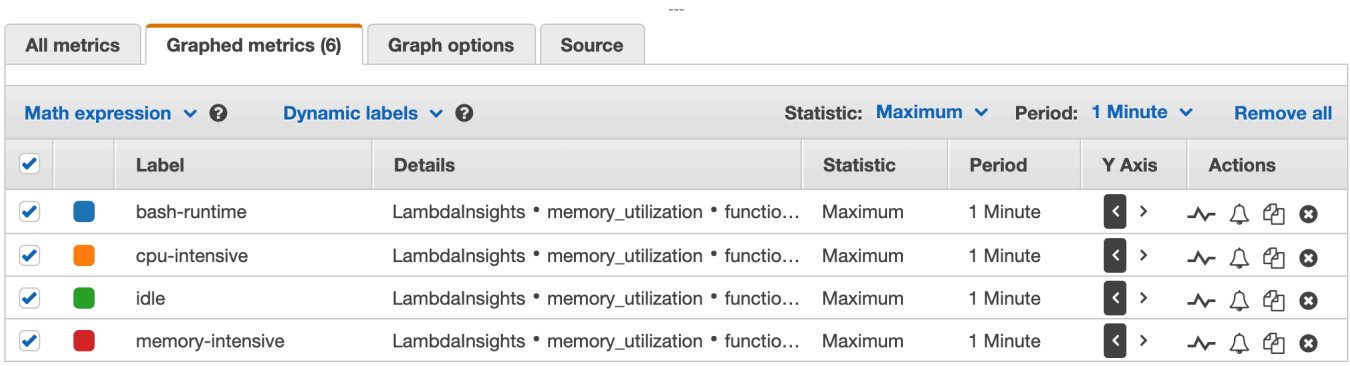
   La vue à fonction unique s'ouvre avec les métriques d'exécution de la fonction d'événement.



3. Dans le volet Memory Usage (Utilisation de la mémoire) sélectionnez les trois points verticaux, puis choisissez View in metrics (Afficher dans les métriques) pour ouvrir le tableau de bord Metrics (Métriques).



4. Dans l'onglet Mesures graphiques, dans la colonne Actions, choisissez la première icône pour activer la détection des anomalies pour la fonction d'événement.



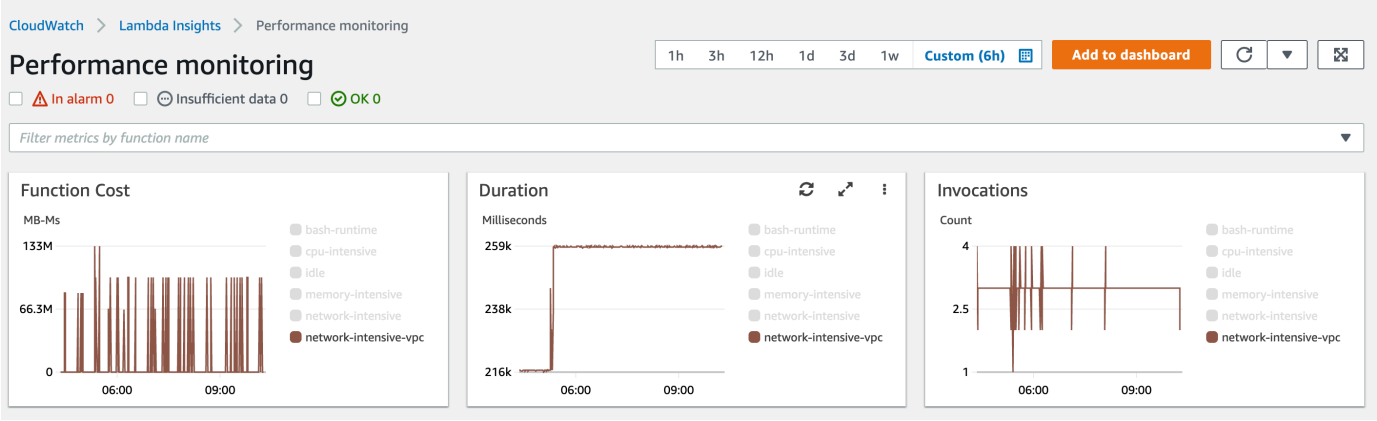
Pour plus d'informations, consultez la section Utilisation de la détection des CloudWatch anomalies.

Exemple de flux de travail utilisant des requêtes pour résoudre les problèmes liés à une fonction événementielle

Vous pouvez utiliser la vue à fonction unique du tableau de bord Lambda Insights pour identifier la cause première d'un pic de durée de la fonction d'événement. Par exemple, si la vue d'ensemble multifonctions indique une augmentation importante de la durée de la fonction d'événement, vous pouvez faire une pause ou choisir chaque fonction d'événement dans le volet Durée pour déterminer quelle fonction d'événement est à l'origine de cette augmentation. Vous pouvez ensuite accéder à la vue de fonction unique et consulter les journaux d'application pour déterminer la cause principale.

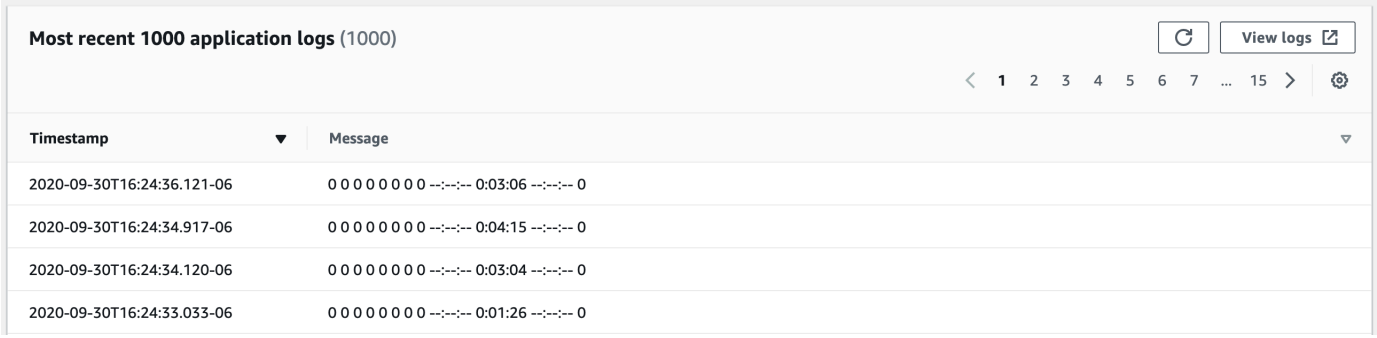
Pour exécuter des requêtes sur une fonction d'événement

1. Ouvrez la Multi-functionpage dans la CloudWatch console.
2. Dans le volet Durée choisissez votre fonction pour filtrer les métriques de durée.

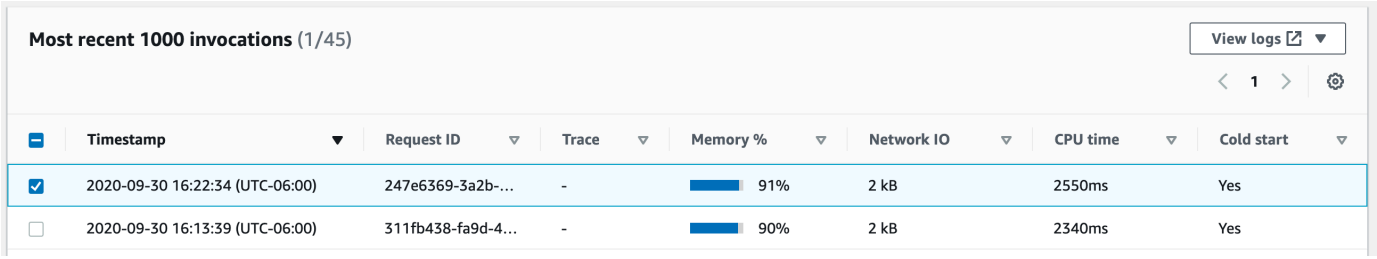


3. Ouvrez la Single-functionpage.

4. Choisissez la liste déroulante Filter metrics by function name (Filtrer les métriques par nom de fonction), puis choisissez votre fonction.
5. Pour afficher les 1000 journaux d'application les plus récents, choisissez l'onglet Application logs (Journaux d'application).
6. Examinez l'horodatage et le message pour identifier la demande d'invocation que vous souhaitez résoudre.

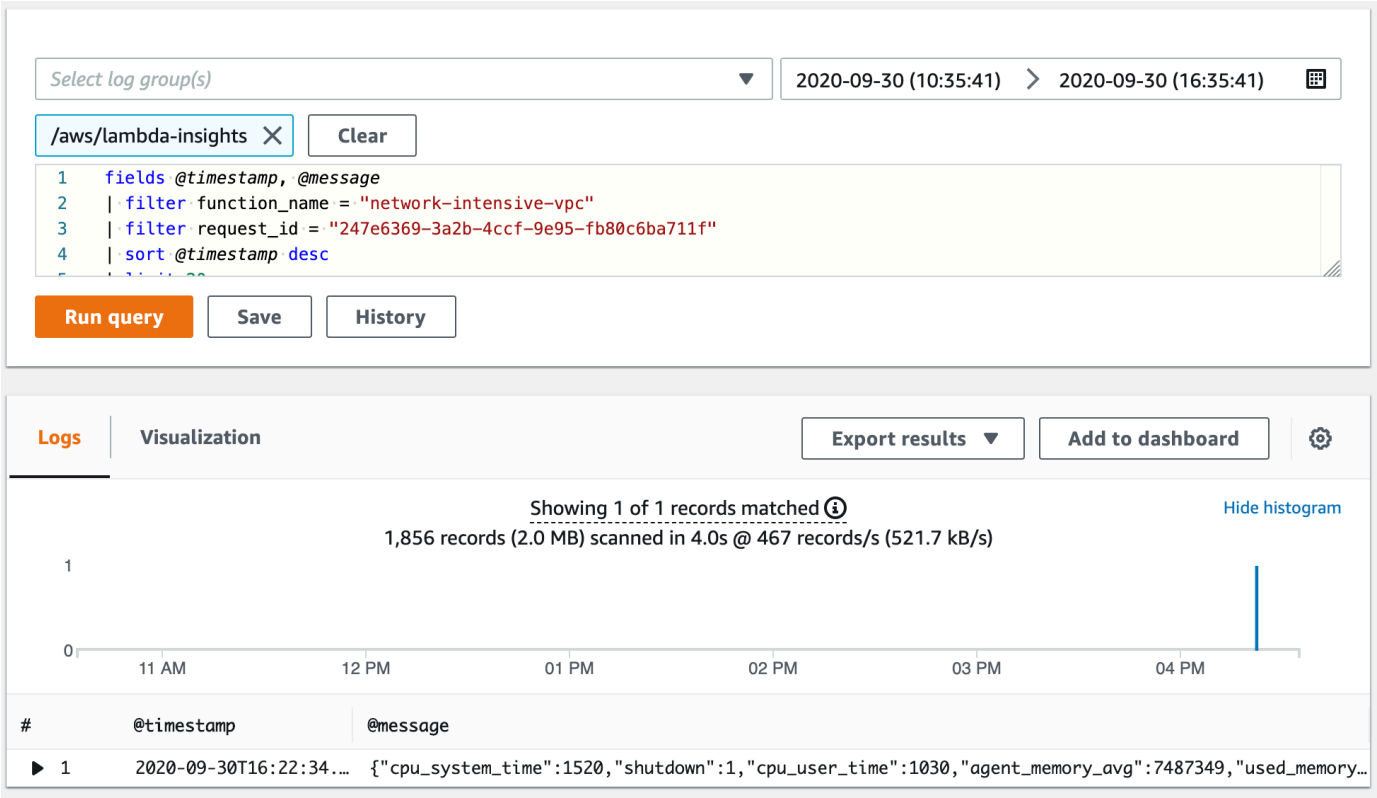


7. Pour afficher les Most recent 1000 invocations (1000 appels les plus récents), choisissez l'onglet Appels.
8. Sélectionnez l'horodatage ou le message pour la demande d'invocation que vous souhaitez résoudre.



9. Choisissez la liste déroulante Afficher les journaux, puis Afficher les journaux de performance.

   Une requête générée automatiquement pour votre fonction événementielle s'ouvre dans le tableau de bord Logs Insights.
10. Choisissez Exécuter la requête pour générer un message Journaux pour la demande d'invocation.



Quelle est la prochaine étape ?

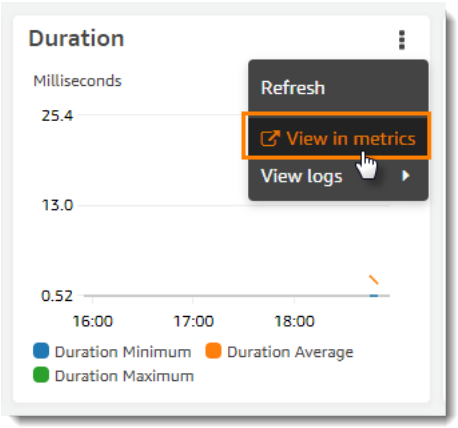
- Découvrez comment créer un tableau de bord CloudWatch Logs dans la section Créer un tableau de bord du guide de CloudWatch l'utilisateur Amazon.
- Découvrez comment ajouter des requêtes à un tableau de bord CloudWatch Logs dans Ajouter une requête au tableau de bord ou Exporter les résultats des requêtes dans le guide de CloudWatch l'utilisateur Amazon.

Surveillance des applications Lambda

La section Applications de la console Lambda inclut un onglet Monitoring dans lequel vous pouvez consulter un tableau de CloudWatch bord Amazon contenant des métriques agrégées pour les ressources de votre application.

Pour surveiller une application Lambda

1. Ouvrez la page Applications de la console Lambda.
2. Choisissez Surveillance.
3. Pour afficher plus de détails sur les métriques dans un graphique, choisissez Afficher dans les métriques dans le menu déroulant.



   Le graphique s'affiche dans un nouvel onglet, avec les métriques correspondantes répertoriées sous le graphique. Vous pouvez personnaliser votre affichage de ce graphique, en modifiant les métriques et les ressources affichées, les statistiques, la période, et d'autres facteurs, afin de mieux comprendre la situation actuelle.

Par défaut, la console Lambda affiche un tableau de bord de base. Vous pouvez personnaliser cette page en ajoutant un ou plusieurs CloudWatch tableaux de bord Amazon à votre modèle d'application avec le type de ressource AWS::CloudWatch::Dashboard. Lorsque votre modèle inclut un ou plusieurs tableaux de bord, la page affiche vos tableaux de bord à la place du tableau de bord par défaut. Vous pouvez basculer entre les tableaux de bord avec le menu déroulant en haut à droite de la page. L'exemple suivant crée un tableau de bord avec un seul widget qui représente graphiquement le nombre d'invocations d'une fonction d'événement nommée. `my-function`

Example Modèle de tableau de bord Event Function

```
Resources:
  MyDashboard:
    Type: AWS::CloudWatch::Dashboard
    Properties:
      DashboardName: my-dashboard
      DashboardBody: |
        {
            "widgets": [
                {
                    "type": "metric",
                    "width": 12,
                    "height": 6,
                    "properties": {
                        "metrics": [
                            [
                                "AWS/Lambda",
                                "Invocations",
                                "FunctionName",
                                "my-function",
                                {
                                    "stat": "Sum",
                                    "label": "MyFunction"
                                }
                            ],
                            [
                                {
                                    "expression": "SUM(METRICS())",
                                    "label": "Total Invocations"
                                }
                            ]
                        ],
                        "region": "us-east-1",
                        "title": "Invocations",
                        "view": "timeSeries",
                        "stacked": false
                    }
                }
            ]
        }
```

Pour plus d'informations sur la création de CloudWatch tableaux de bord et de widgets, consultez la section Structure et syntaxe du corps du tableau de bord dans le Amazon CloudWatch API Reference.

Surveillez les performances des applications avec Amazon CloudWatch Application Signals

Amazon CloudWatch Application Signals est une solution de surveillance des performances des applications (APM) qui permet aux développeurs et aux opérateurs de surveiller l'état et les performances de leurs applications sans serveur créées à l'aide de Lambda. Vous pouvez activer les signaux d'application en un clic depuis la console Lambda, et vous n'avez pas besoin d'ajouter de code d'instrumentation ou de dépendances externes à votre fonction d'événement Lambda. Après avoir activé Application Signals, vous pouvez consulter toutes les mesures et traces collectées dans la CloudWatch console. Cette page explique comment activer et afficher les données de télémétrie de la vigie applicative pour vos applications.

Rubriques

- Mode d’intégration de la vigie applicative à Lambda
- Tarification
- Environnements d'exécution pris en charge
- Activation de la vigie applicative dans la console Lambda
- Utilisation du tableau de bord de la vigie applicative

Mode d’intégration de la vigie applicative à Lambda

Application Signals instrumente automatiquement vos fonctions d'événement Lambda à l'aide des bibliothèques AWS Distro for OpenTelemetry (ADOT) améliorées, fournies via une couche Lambda. La vigie applicative lit les données collectées par la couche et génère des tableaux de bord contenant des indicateurs de performance clés pour vos applications.

Vous pouvez attacher cette couche en un clic en activant la vigie applicative dans la console Lambda. Lorsque vous activez la vigie applicative à partir de la console, Lambda effectue les opérations suivantes en votre nom :

- Met à jour le rôle d'exécution de votre fonction d'événement pour inclure le`CloudWatchLambdaApplicationSignalsExecutionRolePolicy`. Cette politique fournit un accès en écriture AWS X-Ray et aux groupes de CloudWatch journaux utilisés pour les signaux d'application.
- Ajoute une couche à votre fonction d'événement qui instrument automatiquement la fonction d'événement pour capturer des données de télémétrie telles que les demandes, la disponibilité, la

latence, les erreurs et les défauts. Pour garantir le bon fonctionnement des signaux d'application, supprimez tout code d'instrumentation du X-Ray SDK existant de votre fonction d'événement. Le code d'instrumentation personnalisé du X-Ray SDK peut interférer avec l'instrumentation fournie par la couche.

- Ajoute la variable d'`AWS_LAMBDA_EXEC_WRAPPER`environnement à votre fonction d'événement et définit sa valeur sur`/opt/otel-instrument`. Cette variable d'environnement modifie le comportement de démarrage de votre fonction d'événement afin d'utiliser la couche Application Signals. Elle est requise pour une instrumentation appropriée. Si cette variable d'environnement existe déjà, assurez-vous qu'elle est définie sur la valeur adéquate.

Tarification

L'utilisation de signaux d'application pour vos fonctions d'événements Lambda entraîne des coûts. Pour plus d'informations sur les tarifs, consultez CloudWatch les tarifs Amazon.

Environnements d'exécution pris en charge

L'intégration de la vigie applicative à Lambda fonctionne avec les environnements d'exécution suivants :

- .NET 8
- Java 11
- Java 17
- Java 21
- Python 3.10
- Python 3.11
- Python 3.12
- Python 3.13
- Node.js 18,x
- Node.js 20,x
- Node.js 22,x

Activation de la vigie applicative dans la console Lambda

Vous pouvez activer les signaux d'application sur n'importe quelle fonction d'événement Lambda existante à l'aide d'un environnement d'exécution compatible. Les étapes suivantes expliquent comment activer la vigie applicative en un clic dans la console Lambda.

Pour activer la vigie applicative dans la console Lambda

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez la fonction de votre événement.
3. Cliquez sur l'onglet Configuration.
4. Dans le menu de gauche, sélectionnez Outils de surveillance et d'exploitation.
5. Dans le volet Outils de surveillance supplémentaires, choisissez Modifier.
6. Sous Signaux CloudWatch d'application et sous Signaux d'application, sélectionnez Activer. AWS X-Ray
7. Cliquez sur Enregistrer.

Si c'est la première fois que vous activez les signaux d'application pour votre fonction d'événement, vous devez également effectuer une configuration unique de découverte de service pour les signaux d'application dans la CloudWatch console. Une fois que vous avez terminé cette configuration unique de découverte de service, Application Signals découvre automatiquement toutes les fonctions d'événement Lambda supplémentaires pour lesquelles vous activez les signaux d'application, dans toutes les régions.

> **Note**
>
> Une fois que vous avez invoqué votre fonction d'événement mise à jour, les données de service peuvent prendre jusqu'à 10 minutes pour commencer à apparaître dans le tableau de bord des signaux d'application de la CloudWatch console.

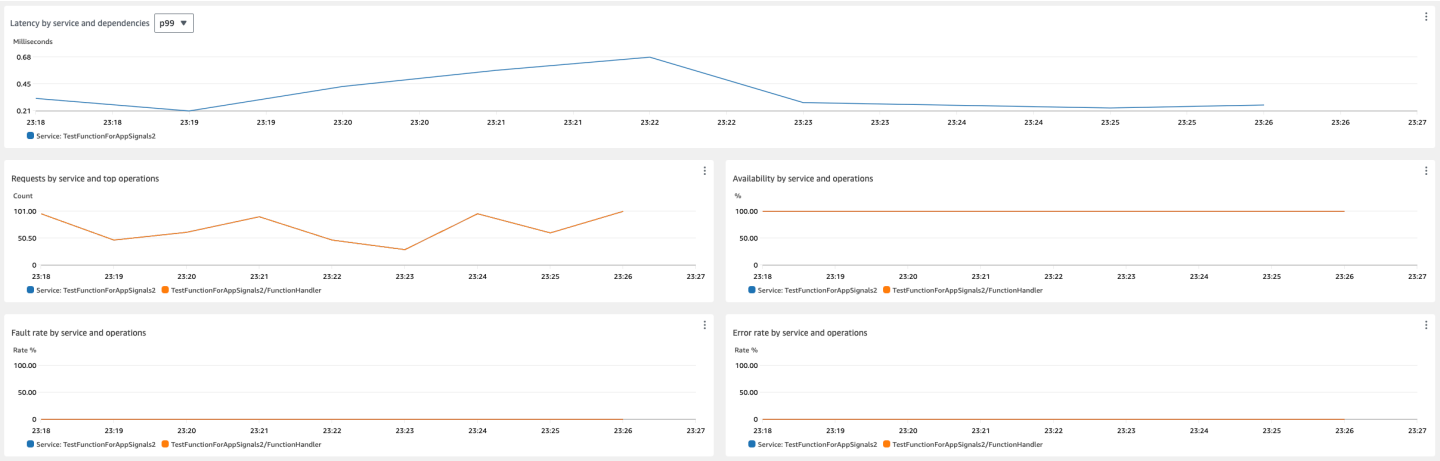
Utilisation du tableau de bord de la vigie applicative

Après avoir activé les signaux d'application pour votre fonction d'événement, vous pouvez visualiser les métriques de votre application dans la CloudWatch console. Vous pouvez rapidement consulter le tableau de bord de la vigie applicative associé depuis la console Lambda en procédant comme suit :

Pour consulter le tableau de bord des signaux d'application pour votre fonction événementielle

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez la fonction de votre événement.
3. Choisissez l’onglet Surveiller.
4. Cliquez sur le bouton Afficher la vigie applicative. Vous accédez ainsi directement à la vue d'ensemble des signaux d'application pour votre service dans la CloudWatch console.

Par exemple, la capture d'écran suivante montre les mesures relatives à la latence, au nombre de demandes, à la disponibilité, au taux d'erreur et au taux d'erreur pour une fonction événementielle sur une période de 10 minutes.



Pour tirer le meilleur parti de votre intégration à la vigie applicative, vous pouvez créer des objectifs de niveau de service (SLO) pour votre application. Par exemple, vous pouvez créer des SLO de latence pour garantir que votre application répond rapidement aux requêtes des utilisateurs, et des SLO de disponibilité pour suivre la durée de fonctionnement. Les SLO peuvent vous aider à détecter la dégradation des performances ou les pannes avant qu’elles n’affectent vos utilisateurs. Pour plus d'informations, consultez la section Objectifs de niveau de service (SLO) dans le guide de l' CloudWatch utilisateur Amazon.

Déboguer à distance les fonctions d'événement Lambda avec Visual Studio Code

Grâce à la fonction de débogage à distance intégrée au AWS Toolkit for Visual Studio Code, vous pouvez déboguer vos fonctions d'événement Lambda exécutées directement dans le cloud. AWS Cela est utile lorsque vous étudiez des problèmes difficiles à reproduire localement ou à diagnostiquer uniquement à l'aide de journaux.

Grâce au débogage à distance, vous pouvez :

- Définissez des points d'arrêt dans le code de votre fonction d'événement Lambda.
- Exécuter le code étape par étape en temps réel.
- Inspecter les variables et leur état pendant l'exécution.
- Déboguez les fonctions d'événement Lambda déployées sur, y compris celles qui AWS se trouvent dans des VPC ou avec des autorisations IAM spécifiques.

Environnements d'exécution pris en charge

Le débogage à distance est pris en charge pour les environnements d'exécution suivants :

- Python (AL2023)
- Java
- JavaScript/Node.js (AL2023)

> **Note**
>
> Le débogage à distance est pris en charge pour les architectures x86_64 et arm64.

Sécurité et débogage à distance

Le débogage à distance fonctionne dans les limites de sécurité Lambda existantes. Les utilisateurs peuvent associer des couches à une fonction d'événement à l'aide de l'`UpdateFunctionConfiguration`autorisation, qui permet déjà d'accéder aux variables d'environnement et à la configuration de la fonction d'événement. Le débogage à distance ne s'étend pas au-delà de ces autorisations existantes. Il ajoute plutôt des contrôles de sécurité supplémentaires

grâce à un tunneling sécurisé et à une gestion automatique des sessions. En outre, le débogage à distance est une fonctionnalité entièrement contrôlée par le client nécessitant des autorisations et des actions explicites :

- Création d'un tunnel sécurisé IoT : le AWS kit d'outils doit créer un tunnel sécurisé IoT, ce qui n'est possible qu'avec l'autorisation explicite de l'utilisateur`iot:OpenTunnel`.
- Attachement de la couche de débogage et gestion des jetons : le processus de débogage assure la sécurité via les contrôles suivants :
  - La couche de débogage doit être attachée à la fonction d'événement Lambda et ce processus nécessite les autorisations `lambda:UpdateFunctionConfiguration` suivantes : et. `lambda:GetLayerVersion`
  - Mettez à jour le jeton de sécurité (généré par`iot:OpenTunnel`) dans la variable d'environnement Event Function avant chaque session de débogage. Cette étape nécessite également`lambda:UpdateFunctionConfiguration`.
  - Pour des raisons de sécurité, ce jeton est automatiquement pivoté, et la couche de débogage est automatiquement supprimée à la fin de chaque session de débogage et ne peut pas être réutilisée.

> **Note**
>
> Le débogage à distance est pris en charge pour les architectures x86_64 et arm64.

Conditions préalables

Avant de commencer le débogage à distance, vérifiez que vous disposez des éléments suivants :

1. Une fonction d'événement Lambda déployée sur votre AWS compte.
2. AWS Toolkit for Visual Studio Code. Consultez Configuration d' AWS Toolkit for Visual Studio Code pour les instructions d'installation.
3. La version du AWS Toolkit que vous avez installée est 3.69.0 ou ultérieure.
4. AWS informations d'identification configurées dans AWS Toolkit for Visual Studio Code. Pour plus d'informations, consultez Authentification et contrôle d'accès.

Déboguer à distance les fonctions d'événement Lambda

Pour démarrer une session de débogage à distance, procédez comme suit :

1. Ouvrez l' AWS explorateur dans VS Code en sélectionnant l' AWS icône dans la barre latérale gauche.
2. Développez la section Lambda pour voir vos fonctions d'événement.
3. Ouvrez le menu contextuel de la fonction d'événement que vous souhaitez déboguer.
4. Dans le menu contextuel, sélectionnez Invoquer à distance.
5. Dans la fenêtre d'invocation qui s'ouvre, cochez la case Activer le débogage.
6. Cliquez sur Invoquer pour démarrer la session de débogage à distance.

> **Note**
>
> Les fonctions d'événement Lambda ont une limite combinée de 250 Mo pour le code de fonction d'événement et toutes les couches associées. La couche de débogage à distance ajoute environ 40 Mo à la taille de votre fonction d'événement.

Une session de débogage à distance se termine quand vous :

- Choisissez Supprimer la configuration de débogage sur l'écran de configuration de l'invocation à distance.
- Sélectionnez l'icône de déconnexion dans les commandes de débogage de VS Code.
- Sélectionnez le fichier de gestionnaire dans l'éditeur VS Code.

> **Note**
>
> La couche de débogage est automatiquement supprimée après 60 secondes d'inactivité après votre dernière invocation.

Désactiver le débogage à distance

Vous pouvez désactiver cette fonctionnalité de trois manières :

- Refuser les mises à jour de fonction : définissez `lambda:UpdateFunctionConfiguration` sur `deny`.
- Restreindre les autorisations IoT : refuser IoT-related les autorisations
- Bloquer les couches de débogage : refusez `lambda:GetLayerVersion` pour les ARN suivants :
  - `arn:aws:lambda:*:*:layer:LDKLayerX86:*`
  - `arn:aws:lambda:*:*:layer:LDKLayerArm64:*`

> **Note**
>
> La désactivation de cette fonctionnalité empêche l'ajout de la couche de débogage lors des mises à jour de configuration de la fonction d'événement.

Informations supplémentaires

Pour plus d'informations sur l'utilisation de Lambda dans VS Code, reportez-vous à la section Développement de fonctions Lambda localement avec VS Code.

Pour obtenir des instructions détaillées sur le dépannage, les cas d'utilisation avancés et la disponibilité régionale, consultez la section Débogage à distance des fonctions Lambda dans AWS Toolkit for Visual Studio Code le guide de l'utilisateur.

Invoquer Lambda avec des événements provenant d'autres AWS services

Certains Services AWS peuvent appeler directement les fonctions d'événement Lambda à l'aide de déclencheurs. Ces services envoient des événements à Lambda, et la fonction est invoquée aussitôt que l'événement spécifié se produit. Les déclencheurs sont adaptés aux événements discrets et au traitement en temps réel. Lorsque vous créez un déclencheur à l'aide de la console Lambda, celle-ci interagit avec le AWS service correspondant pour configurer la notification d'événement sur ce service. Le déclencheur est en fait stocké et géré par le service qui génère les événements, et non par Lambda.

Les événements sont des données structurées au format JSON. La structure JSON varie en fonction du service qui la génère et du type d'événement, mais elles contiennent toutes les données nécessaires à la fonction pour traiter l'événement.

Outre les appels pilotés par des événements, vous pouvez utiliser Lambda avec Amazon EC2, Apache Kafka autogéré et Kubernetes.

Une fonction d'événement peut avoir plusieurs déclencheurs. Chaque déclencheur agit comme un client qui invoque votre fonction indépendamment, et chaque événement que Lambda transmet à votre fonction contient des données provenant d'un seul déclencheur. Lambda convertit le document d'événement en objet et le transmet à votre gestionnaire de fonctions.

Selon le service, l'invocation pilotée par l'événement peut être synchrone ou asynchrone.

- Pour une invocation synchrone, l'autre service qui génère l'événement attend la réponse de votre fonction. Ce service définit les données que la fonction doit renvoyer dans la réponse. Le service contrôle la stratégie d'erreur, par exemple s'il faut réessayer les erreurs.
- Pour l'invocation asynchrone, Lambda place l'événement dans une file d'attente avant de le transmettre à votre fonction. Lorsque Lambda met l'événement en file d'attent, il envoie immédiatement une réponse de réussite au service qui a généré l'événement. Une fois que la fonction a traité l'événement, Lambda ne renvoie pas de réponse au service générateur d'événements.

Création d'un déclencheur

La manière la plus simple de créer un déclencheur consiste à utiliser la console Lambda. Lorsque vous créez un déclencheur à l'aide de la console, Lambda ajoute automatiquement les autorisations requises à la politique basée sur les ressources de la fonction d'événement.

Pour créer un déclencheur à l'aide de la console Lambda

1. Ouvrez la page Event Functions de la console Lambda.
2. Sélectionnez la fonction pour laquelle vous souhaitez créer un déclencheur.
3. Dans le volet de Présentation de la fonction, choisissez Ajouter un déclencheur.
4. Sélectionnez le AWS service pour lequel vous souhaitez appeler votre fonction.
5. Renseignez les options dans le volet de configuration du déclencheur et choisissez Ajouter. En fonction de la fonction Service AWS que vous choisissez d'appeler, les options de configuration du déclencheur sont différentes.

Services pouvant invoquer des fonctions d'événement Lambda

Le tableau suivant répertorie les services qui peuvent invoquer les fonctions d'événement Lambda.

Service	Méthode d'invocation
Streaming géré par Amazon pour Apache Kafka	Mappage des sources d'événements
Self-managed Apache Kafka	Mappage des sources d'événements
Amazon API Gateway	Event-driven; invocation synchrone
AWS CloudFormation	Event-driven; invocation asynchrone
Amazon CloudWatch Logs	Event-driven; invocation asynchrone
AWS CodeCommit	Event-driven; invocation asynchrone
AWS CodePipeline	Event-driven; invocation asynchrone
Amazon Cognito	Event-driven; invocation synchrone
AWS Config	Event-driven; invocation asynchrone
Connect le client	Event-driven; invocation synchrone
Amazon DocumentDB	Mappage des sources d'événements
Amazon DynamoDB	Mappage des sources d'événements
Elastic Load Balancing (Application Load Balancer)	Event-driven; invocation synchrone
EventBridge	Event-driven; appel asynchrone (bus d'événements et règles), appel synchrone ou asynchrone (canaux)
Amazon EventBridge Scheduler	Event-driven (basé sur le temps) ; invocation asynchrone
AWS IoT	Event-driven; invocation asynchrone

Service	Méthode d'invocation
Amazon Kinesis	Mappage des sources d'événements
Amazon Data Firehose	Event-driven; invocation synchrone
Amazon Lex	Event-driven; invocation synchrone
Amazon MQ	Mappage des sources d'événements
Amazon Simple Email Service	Event-driven; invocation asynchrone
Amazon Simple Notification Service	Event-driven; invocation asynchrone
Amazon Simple Queue Service	Mappage des sources d'événements
Amazon Simple Storage Service (Amazon S3)	Event-driven; invocation asynchrone
Amazon Simple Storage Service Batch	Event-driven; invocation synchrone
Secrets Manager	Rotation des secrets
AWS Step Functions	Event-driven; invocation synchrone ou asynchrone
Amazon VPC Lattice	Event-driven; invocation synchrone

Utilisation de Lambda avec Apache Kafka

Lambda prend en charge Apache Kafka en tant que source d'événement. Apache Kafka est une plateforme open source de diffusion en continu d'événements conçue pour gérer des pipelines de données en temps réel à haut débit et des applications de diffusion en continu. Il existe deux méthodes principales pour utiliser Lambda avec Apache Kafka :

- the section called "MSK" — Amazon Managed Streaming pour Apache Kafka (Amazon MSK) est un service entièrement géré par AWS. Amazon MSK permet d'automatiser la gestion de votre infrastructure Kafka, notamment le provisionnement, l'application de correctifs et la mise à l'échelle.
- the section called "Self-managed Apache Kafka" — Dans AWS terminologie, un cluster autogéré comprend des entités non AWS clusters Kafka hébergés. Par exemple, vous pouvez toujours utiliser Lambda avec un cluster Kafka hébergé par un autre AWS un fournisseur de cloud tel que Cloud Confluent ou Panda roux.

Lorsque vous choisissez entre Amazon MSK et Apache Kafka autogéré, tenez compte de vos besoins opérationnels et de vos exigences en matière de contrôle. Amazon MSK est un meilleur choix si vous le souhaitez AWS pour vous aider à gérer rapidement une configuration Kafka évolutive et prête pour la production avec un minimum de frais opérationnels. Cette solution simplifie la sécurité, la surveillance et la haute disponibilité, vous permettant ainsi de vous concentrer sur le développement d'applications plutôt que sur la gestion de l'infrastructure. D'autre part, Apache Kafka autogéré est mieux adapté aux cas d'utilisation exécutés sur des applications qui ne sont pas des AWS environnements hébergés, y compris les clusters sur site.

Rubriques

- Utilisation de Lambda avec Amazon MSK
- Utilisation de Lambda avec Apache Kafka autogéré
- Modes de mise à l'échelle des sondeurs d'événements Apache Kafka dans Lambda
- Positions de départ des interrogations et flux Apache Kafka dans Lambda
- Interroger les sujets de Kafka en mode file d'attente
- ID de groupe de consommateurs personnalisable dans Lambda
- Filtrage des événements provenant d'Amazon MSK et sources d'événements Apache Kafka autogéré
- Utilisation de registres de schémas avec les sources d'événements Kafka dans Lambda
- Traitement à faible latence pour les sources d'événements Kafka

- Configuration des contrôles de gestion des erreurs pour les sources d'événements Kafka
- Capture de lots supprimés pour des sources d’événement Amazon MSK et Apache Kafka autogéré
- Utiliser un sujet Kafka comme destination en cas d'échec
- Journalisation du mappage des sources d'événements Kafka
- Résolution des erreurs de mappage des sources d’événements Kafka

Utilisation de Lambda avec Amazon MSK

Amazon Managed Streaming for Apache Kafka (Amazon MSK) est un service entièrement géré qui vous permet de créer et d'exécuter des applications qui utilisent Apache Kafka pour traiter des données en streaming. Amazon MSK simplifie la configuration, la mise à l'échelle et la gestion des clusters Kafka. Amazon MSK facilite également la configuration de votre application pour plusieurs zones de disponibilité et pour des raisons de sécurité avec Gestion des identités et des accès AWS (IAM).

Ce chapitre explique comment utiliser un cluster Amazon MSK comme source d'événements pour votre fonction d'événement Lambda. Le processus général d'intégration d'Amazon MSK à Lambda comprend les étapes suivantes :

1. Configuration du cluster et du réseau : configurez d'abord votre cluster Amazon MSK. Cela inclut la configuration réseau correcte pour permettre à Lambda d'accéder à votre cluster.
2. Configuration du mappage des sources d'événements : créez ensuite la ressource de mappage des sources d'événements dont Lambda a besoin pour connecter de façon sécurisée votre cluster Amazon MSK à votre fonction.
3. Configuration de la fonction événementielle et des autorisations — Enfin, assurez-vous que votre fonction est correctement configurée et qu'elle dispose des autorisations nécessaires dans son rôle d'exécution.

> **Note**
>
> Vous pouvez désormais créer et gérer vos mappages de sources d'événements Amazon MSK directement depuis la console Lambda ou Amazon MSK. Les deux consoles offrent la possibilité de gérer automatiquement la configuration des autorisations de rôle d'exécution Lambda nécessaires pour un processus de configuration plus rationalisé.

Pour des exemples expliquant comment configurer une intégration Lambda avec un cluster Amazon MSK, consultez les sections the section called "didacticiel" Utilisation d'Amazon MSK comme source d'événements AWS Lambda sur le blog AWS Compute et Intégration d'Amazon MSK Lambda dans les Amazon MSK Labs.

Rubriques

- Exemple d'évènement

- Configuration de votre cluster Amazon MSK et de votre réseau Amazon VPC pour Lambda
- Configuration des autorisations Lambda pour les mappages de sources d'événements Amazon MSK
- Configuration de source d’événements Amazon MSK pour Lambda
- Tutoriel : Utilisation d'un mappage de source d'événements Amazon MSK pour appeler une fonction d'événement Lambda

Exemple d’évènement

Lambda envoie le lot de messages dans le paramètre d'événement lorsqu'il appelle votre fonction d'événement. La charge utile d’un événement contient un tableau de messages. Chaque élément de tableau contient des détails de la rubrique Amazon MSK et un identifiant de partition, ainsi qu’un horodatage et un message codé en base 64.


```
{
   "eventSource":"aws:kafka",
   "eventSourceArn":"arn:aws:kafka:us-east-1:123456789012:cluster/
vpc-2priv-2pub/751d2973-a626-431c-9d4e-d7975eb44dd7-2",
   "bootstrapServers":"b-2.demo-cluster-1.a1bcde.c1.kafka.us-
east-1.amazonaws.com:9092,b-1.demo-cluster-1.a1bcde.c1.kafka.us-
east-1.amazonaws.com:9092",
   "records":{
      "mytopic-0":[
         {
            "topic":"mytopic",
            "partition":0,
            "offset":15,
            "timestamp":1545084650987,
            "timestampType":"CREATE_TIME",
            "key":"abcDEFghiJKLmnoPQRstuVWXyz1234==",
            "value":"SGVsbG8sIHRoaXMgaXMgYSB0ZXN0Lg==",
            "headers":[
               {
                  "headerKey":[
                     104,
                     101,
                     97,
                     100,
                     101,
                     114,
                     86,
```

```
                    97,
                    108,
                    117,
                    101
                ]
            }
        ]
    }
  ]
 }
}
```

Configuration de votre cluster Amazon MSK et de votre réseau Amazon VPC pour Lambda

Pour connecter votre fonction d' AWS Lambda événement à votre cluster Amazon MSK, vous devez configurer correctement votre cluster et l'Amazon Virtual Private Cloud (VPC) dans lequel il réside. Cette page décrit comment configurer votre cluster et votre VPC. Si votre cluster et votre VPC sont déjà correctement configurés, consultez the section called “Configurer une source d’événements” pour configurer le mappage des sources d’événements.

Rubriques

- Présentation des exigences de configuration réseau pour les intégrations Lambda et MSK
- Configuration d’une passerelle NAT pour une source d’événements MSK
- Configuration AWS PrivateLink points de terminaison pour une source d'événements MSK

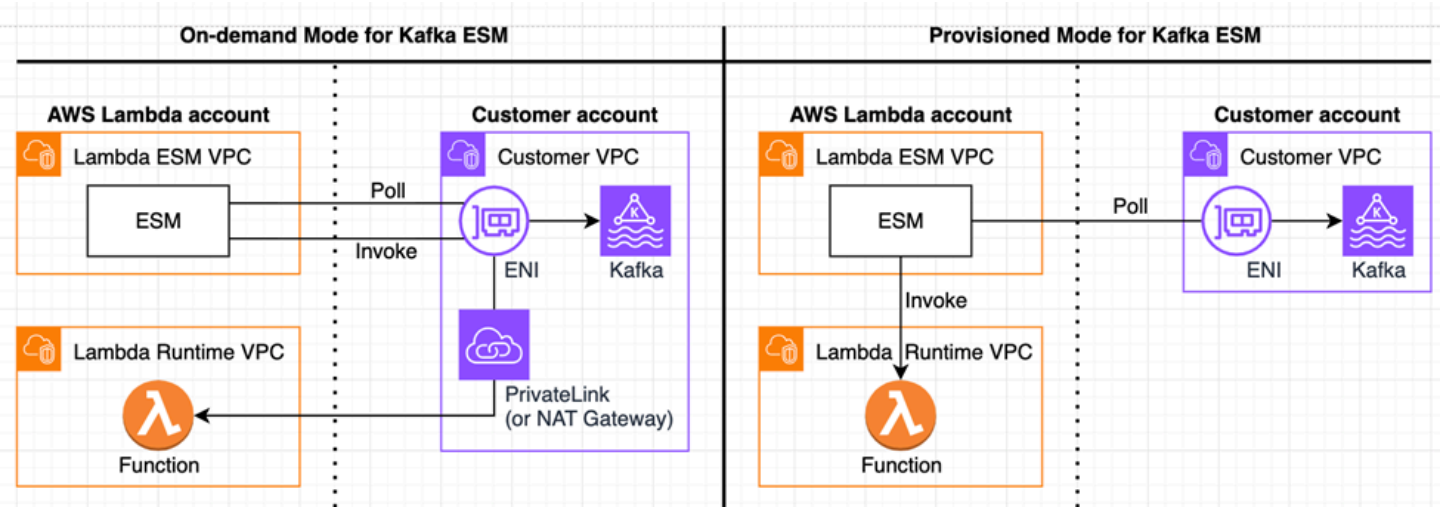
Présentation des exigences de configuration réseau pour les intégrations Lambda et MSK

La configuration réseau requise pour une intégration Lambda et MSK dépend de l’architecture réseau de votre application. Trois ressources principales sont impliquées dans cette intégration : le cluster Amazon MSK, la fonction d'événement Lambda et le mappage des sources d'événements Lambda. Chacune de ces ressources réside dans un VPC différent :

- Votre cluster Amazon MSK réside généralement dans un sous-réseau privé d’un VPC que vous gérez.
- Votre fonction d'événement Lambda réside dans un VPC AWS géré appartenant à Lambda.
- Le mappage de votre source d'événements Lambda réside dans un autre VPC AWS géré appartenant à Lambda, distinct du VPC qui contient votre fonction.

Le mappage des sources d'événements est la ressource intermédiaire entre le cluster MSK et la fonction d'événement Lambda. Le mappage des sources d'événements effectue deux tâches principales. Tout d'abord, il interroge votre cluster MSK à la recherche de nouveaux messages. Ensuite, il invoque votre fonction d'événement Lambda avec ces messages. Étant donné que ces trois ressources se trouvent dans des VPC différents, les opérations d'interrogation et d'invocation nécessitent des appels réseau entre VPC.

Les exigences de configuration réseau pour votre mappage des sources d'événements varient selon qu'il utilise le mode provisionné ou le mode à la demande, comme le montre le schéma suivant :



La façon dont le mappage des sources d'événements Lambda interroge votre cluster MSK à la recherche de nouveaux messages est la même dans les deux modes. Pour établir une connexion entre votre mappage des sources d'événements et votre cluster MSK, Lambda crée une ENI Hyperplane (ou réutilise une ENI existante, si disponible) dans votre sous-réseau privé afin d'établir une connexion sécurisée. Comme illustré dans le schéma, cet hyperplan ENI utilise la configuration du sous-réseau et du groupe de sécurité de votre cluster MSK, et non votre fonction d'événement Lambda.

Après avoir interrogé le message du cluster, la façon dont Lambda invoque votre fonction est différente dans chaque mode :

- En mode provisionné, Lambda gère automatiquement la connexion entre le VPC du mappage des sources d'événements et le VPC de la fonction. Vous n'avez donc pas besoin de composants réseau supplémentaires pour appeler correctement votre fonction.
- En mode à la demande, le mappage de votre source d'événements Lambda appelle votre fonction en utilisant un chemin passant par votre VPC géré par le client. Pour cette raison, vous devez configurer soit une passerelle NAT dans le sous-réseau public de votre VPC, soit des points

de terminaison AWS PrivateLink dans le sous-réseau privé du VPC qui fournissent un accès à Lambda, AWS Security Token Service (STS) et éventuellement AWS Secrets Manager. La configuration correcte de l'une ou l'autre de ces options permet d'établir une connexion entre votre VPC et le Lambda-managed VPC d'exécution, ce qui est nécessaire pour appeler votre fonction.

Une passerelle NAT permet aux ressources de votre sous-réseau privé d'accéder à l'Internet public. L'utilisation de cette configuration signifie que votre trafic traverse Internet avant d'appeler la fonction d'événement Lambda. AWS PrivateLink les points de terminaison permettent aux sous-réseaux privés de se connecter en toute sécurité à AWS des services ou à d'autres ressources VPC privées sans passer par l'Internet public. Consultez the section called “Configuration d’une passerelle NAT pour une source d’événements MSK” ou the section called “Configuration AWS PrivateLink points de terminaison pour une source d'événements MSK” pour en savoir plus sur la façon de configurer ces ressources.

Jusqu'à présent, nous avons supposé que votre cluster MSK résidait dans un sous-réseau privé au sein de votre VPC, ce qui est le cas le plus courant. Toutefois, même si votre cluster MSK se trouve dans un sous-réseau public au sein de votre VPC, vous devez configurer des points de terminaison AWS PrivateLink pour permettre une connexion sécurisée. Le tableau suivant résume les exigences de configuration réseau en fonction de la façon dont vous configurez votre cluster MSK et du mappage des sources d’événements Lambda :

Emplacement du cluster MSK (dans un VPC géré par le client)	Mode de mise à l’échelle du mappage des sources d’événements Lambda	Configuration réseau requise
Sous-réseau privé	On-demand mode	Passerelle NAT (dans le sous-réseau public de votre VPC) ou AWS PrivateLink points de terminaison (dans le sous-réseau privé de votre VPC) pour permettre l'accès à Lambda, et AWS STSéventuellement à Secrets Manager.
Public subnet	On-demand mode	AWS PrivateLink points de terminaison (dans le sous-réseau public de votre VPC) pour

Emplacement du cluster MSK (dans un VPC géré par le client)	Mode de mise à l'échelle du mappage des sources d'événements Lambda	Configuration réseau requise
		permettre l'accès à Lambda et, éventuellement AWS STS, à Secrets Manager.
Sous-réseau privé	Mode alloué	Aucune
Public subnet	Mode alloué	Aucune

En outre, les groupes de sécurité associés à votre cluster MSK doivent autoriser le trafic sur les bons ports. Vérifiez que les règles de groupe de sécurité suivantes sont configurées :

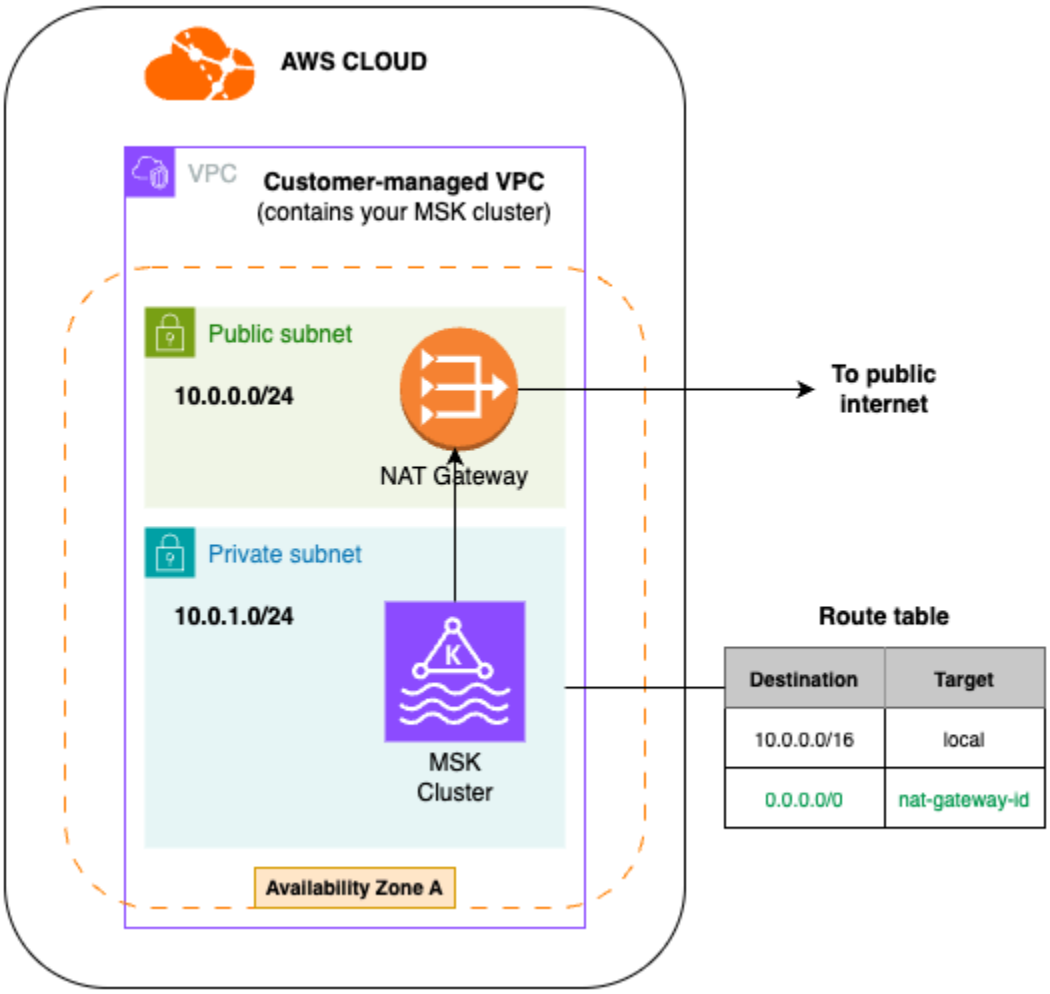
- Règles entrantes : autorisez tout le trafic sur le port d'agent par défaut. Le port utilisé par MSK dépend du type d'authentification sur le cluster : `9098` pour l'authentification IAM SASL/SCRAM, `9096` pour et `9094` pour TLS. Vous pouvez également utiliser une règle de groupe de sécurité avec référence circulaire pour autoriser l'accès à partir d'instances appartenant au même groupe de sécurité.
- Règles de sortie : autorisez tout le trafic sur le port `443` pour les destinations externes si votre fonction doit communiquer avec d'autres AWS services. Vous pouvez également utiliser une règle de groupe de sécurité à référencement automatique pour limiter l'accès au courtier si vous n'avez pas besoin de communiquer avec d'autres AWS services.
- Règles relatives au point de terminaison Amazon VPC : si vous utilisez un point de terminaison Amazon VPC, le groupe de sécurité associé au point de terminaison doit autoriser le trafic entrant sur le port en `443` provenance du groupe de sécurité du cluster.

Configuration d'une passerelle NAT pour une source d'événements MSK

Vous pouvez configurer une passerelle NAT pour permettre au mappage de votre source d'événements d'interroger les messages de votre cluster et d'invoquer la fonction d'événement en utilisant un chemin via votre VPC. Cela n'est nécessaire que si votre mappage des sources d'événements utilise le mode à la demande et que votre cluster réside dans un sous-réseau privé de votre VPC. Si votre cluster réside dans un sous-réseau public de votre VPC, ou si le mappage des sources d'événements utilise le mode provisionné, vous n'avez pas besoin de configurer de passerelle NAT.

Une passerelle NAT permet aux ressources d'un sous-réseau privé d'accéder à l'Internet public. Si vous avez besoin d'une connectivité privée à Lambda, consultez plutôt the section called "Configuration AWS PrivateLink points de terminaison pour une source d'événements MSK".

Après avoir configuré votre passerelle NAT, vous devez configurer les tables de routage appropriées. Cela permet au trafic provenant de votre sous-réseau privé d'être acheminé vers l'Internet public via la passerelle NAT.



Les étapes suivantes vous guident dans la mise en réseau d'une passerelle NAT à l'aide de la console. Si nécessaire, répétez ces étapes pour chaque zone de disponibilité (AZ).

Configurer une passerelle NAT et un routage approprié (console)

1. Suivez les étapes de Créer une passerelle NAT, en notant ce qui suit :
   - Les passerelles NAT doivent toujours résider dans un sous-réseau public. Créez des passerelles NAT avec une connectivité publique.

- Si votre cluster MSK est répliqué à travers plusieurs AZ, créez une passerelle NAT par AZ. Par exemple, dans chaque AZ, votre VPC doit avoir un sous-réseau privé contenant votre cluster et un sous-réseau public contenant votre passerelle NAT. Pour une configuration avec trois AZ, vous aurez trois sous-réseaux privés, trois sous-réseaux publics et trois passerelles NAT.

2. Après avoir créé votre passerelle NAT, ouvrez la console Amazon VPC et choisissez Tables de routage dans le menu de gauche.
3. Choisissez Créer une table de routage.
4. Associez cette table de routage au VPC contenant votre cluster MSK. Vous pouvez éventuellement saisir un nom pour votre table de routage.
5. Choisissez Créer une table de routage.
6. Choisissez la table de routage que vous venez de créer.
7. Sur l'onglet Associations de sous-réseau, choisissez Modifier les associations de sous-réseau.

   - Associez cette table de routage au sous-réseau privé contenant votre cluster MSK.

8. Choisissez Edit routes (Modifier des routes).
9. Choisissez Ajouter une route :

   1. Pour Destination, choisissez `0.0.0.0/0`.
   2. Pour Cible, choisissez Passerelle NAT.
   3. Dans la zone de recherche, choisissez la passerelle NAT que vous avez créée à l'étape 1. Il doit s'agir de la passerelle NAT située dans la même AZ que le sous-réseau privé contenant votre cluster MSK (le sous-réseau privé que vous avez associé à cette table de routage à l'étape 6).

10. Cliquez sur Enregistrer les modifications.

Configuration AWS PrivateLink points de terminaison pour une source d'événements MSK

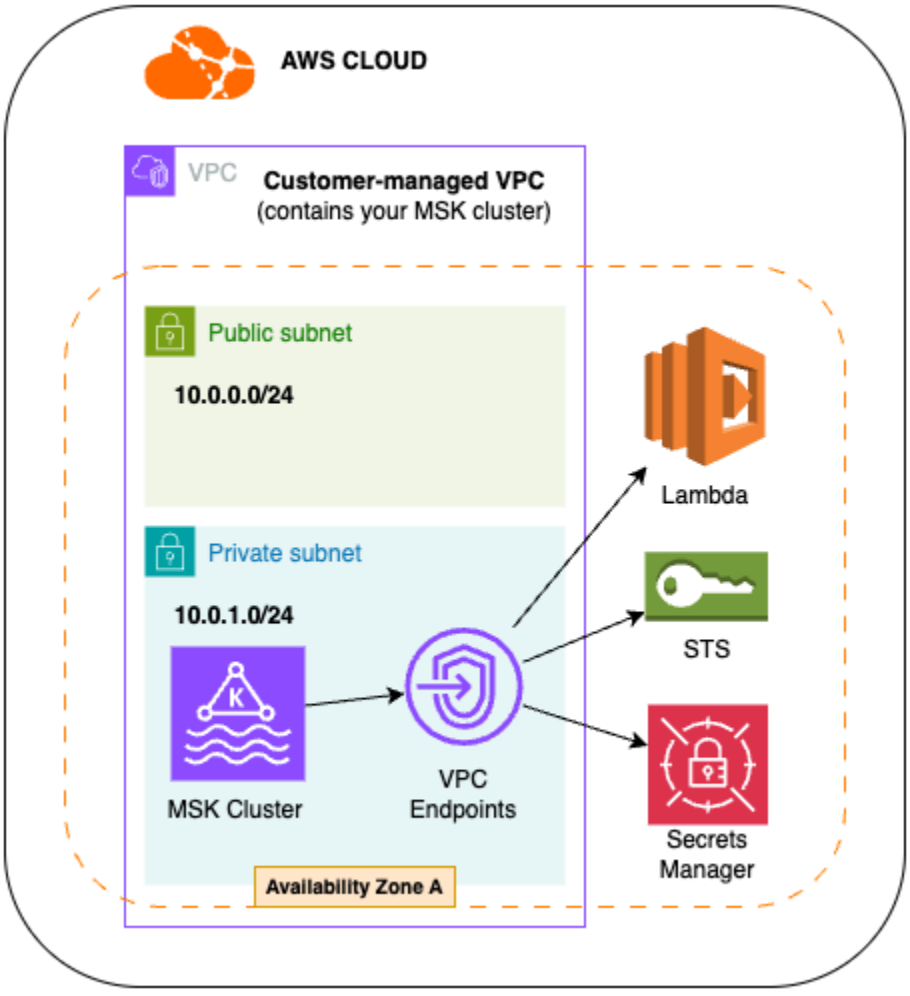
Vous pouvez configurer les AWS PrivateLink points de terminaison pour interroger les messages de votre cluster et appeler la fonction en utilisant un chemin via votre VPC. Ces points de terminaison devraient permettre à votre cluster MSK d'accéder à ce qui suit :

- Le service Lambda
- AWS Security Token Service (STS)
- Éventuellement le service AWS Secrets Manager. Il est nécessaire si le secret requis pour l'authentification du cluster est stocké dans Secrets Manager.

La configuration des PrivateLink points de terminaison n'est requise que si le mappage des sources d'événements utilise le mode à la demande. Si votre mappage des sources d'événements utilise le mode provisionné, Lambda établit les connexions requises pour vous.

PrivateLink les points de terminaison permettent un accès sécurisé et privé aux AWS services. AWS PrivateLink Vous pouvez également configurer une passerelle NAT afin de permettre à votre cluster MSK d'accéder à l'Internet public (voir the section called "Configuration d'une passerelle NAT pour une source d'événements MSK").

Une fois que vous avez configuré vos points de terminaison de VPC, votre cluster MSK devrait disposer d'un accès direct et privé à Lambda, STS et éventuellement Secrets Manager.



Les étapes suivantes vous guident dans la configuration d'un PrivateLink point de terminaison à l'aide de la console. Si nécessaire, répétez ces étapes pour chaque point de terminaison (Lambda, STS, Secrets Manager).

Pour configurer les PrivateLink points de terminaison VPC (console)

1. Ouvrez la console Amazon VPC et choisissez Points de terminaison dans le menu de gauche.
2. Choisissez Créer un point de terminaison.
3. Vous pouvez éventuellement saisir un nom pour votre point de terminaison.
4. Dans Type, sélectionnez Services AWS .
5. Sous Services, commencez à saisir le nom du service. Par exemple, pour créer un point de terminaison pour la connexion à Lambda, saisissez `lambda` dans le champ de recherche.
6. Dans les résultats, vous devriez voir le point de terminaison de service dans la région actuelle. Par exemple, dans la région USA Est (Virginie du Nord), vous devriez voir `com.amazonaws.us-east-2.lambda`. Sélectionnez ce service.
7. Sous Paramètres réseau, sélectionnez le VPC qui contient votre cluster MSK.
8. Sous Sous-réseaux, sélectionnez les AZ dans lesquelles se trouve votre cluster MSK.
   - Pour chaque AZ, sous ID de sous-réseau, choisissez le sous-réseau privé contenant votre cluster MSK.
9. Sous Groupes de sécurité, sélectionnez les groupes de sécurité associés à votre cluster MSK.
10. Choisissez Créer un point de terminaison.

Par défaut, les points de terminaison Amazon VPC disposent de politiques IAM ouvertes qui permettent un accès étendu aux ressources. La meilleure pratique consiste à restreindre ces politiques pour effectuer les actions nécessaires à l'aide de ce point de terminaison. Par exemple, pour votre point de terminaison Secrets Manager, vous pouvez modifier sa politique de telle sorte qu'il autorise uniquement le rôle d'exécution de votre fonction à accéder au secret.

Example Politique de point de terminaison de VPC – Point de terminaison Secrets Manager

```
{
    "Statement": [
        {
            "Action": "secretsmanager:GetSecretValue",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws::iam::123456789012:role/my-role"
                ]
            },
```

```
            "Resource": "arn:aws::secretsmanager:us-west-2:123456789012:secret:my-
secret"
        }
    ]
}
```

Pour les points de terminaison Lambda AWS STS et Lambda, vous pouvez limiter le principal appelant au principal de service Lambda. Cependant, assurez-vous d'utiliser `"Resource": "*"` dans ces politiques.

Example Politique relative aux points de terminaison VPC — AWS STS point de terminaison

```
{
    "Statement": [
        {
            "Action": "sts:AssumeRole",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "lambda.amazonaws.com"
                ]
            },
            "Resource": "*"
        }
    ]
}
```

Example Politique de point de terminaison de VPC – Point de terminaison Lambda

```
{
    "Statement": [
        {
            "Action": "lambda:InvokeFunction",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "lambda.amazonaws.com"
                ]
            },
            "Resource": "*"
        }
    ]
```

```
}
```

Configuration des autorisations Lambda pour les mappages de sources d'événements Amazon MSK

Pour accéder au cluster Amazon MSK, votre fonction d'événement et le mappage de la source de l'événement ont besoin d'autorisations pour effectuer diverses actions de l'API Amazon MSK. Ajoutez ces autorisations au rôle d'exécution de votre fonction. Si vos utilisateurs ont besoin de l'accès, ajoutez les autorisations requises à la stratégie d'identité de l'utilisateur ou du rôle correspondant.

La politique AWSLambdaMSKExecutionRolegérée contient les autorisations minimales requises pour les mappages de sources d'événements Amazon MSK Lambda. Pour simplifier le processus d'autorisation, vous pouvez :

- Associez la politique AWSLambdaMSKExecutionRolegérée à votre rôle d'exécution.
- Laissez la console Lambda générer les autorisations pour vous. Lorsque vous créez un mappage de source d'événement Amazon MSK dans la console, Lambda évalue votre rôle d'exécution et vous avertit si des autorisations sont manquantes. Choisissez Générer des autorisations pour mettre à jour automatiquement votre rôle d'exécution. Cela ne fonctionne pas si vous avez créé ou modifié manuellement vos politiques de rôle d'exécution, ou si les politiques sont associées à plusieurs rôles. Notez que des autorisations supplémentaires peuvent toujours être requises dans votre rôle d'exécution lorsque vous utilisez des fonctionnalités avancées telles que On-Failure Destination ou AWS Glue Schema Registry.

Rubriques

- Autorisations requises
- Autorisations facultatives

Autorisations requises

Votre rôle d'exécution de la fonction d'événement Lambda doit disposer des autorisations requises suivantes pour les mappages de sources d'événements Amazon MSK. Ces autorisations sont incluses dans la politique AWSLambdaMSKExecutionRolegérée.

CloudWatch Autorisations de journalisation

Les autorisations suivantes permettent à Lambda de créer et de stocker des journaux dans Amazon CloudWatch Logs.

- journaux : CreateLogGroup
- journaux : CreateLogStream
- journaux : PutLogEvents

Autorisations du cluster MSK

Les autorisations suivantes permettent à Lambda d'accéder à votre cluster Amazon MSK en votre nom :

- Kafka : DescribeCluster
- Source : V2 DescribeCluster
- Kafka : GetBootstrapBrokers

Nous recommandons d'utiliser kafka : DescribeCluster V2 au lieu de kafka :. DescribeCluster L'autorisation v2 fonctionne à la fois avec les clusters Amazon MSK provisionnés et sans serveur. Vous n'avez besoin que d'une de ces autorisations dans votre politique.

Autorisations VPC

Les autorisations suivantes permettent à Lambda de créer et de gérer des interfaces réseau lors de la connexion à votre cluster Amazon MSK :

- EC2 : CreateNetworkInterface
- EC2 : DescribeNetworkInterfaces
- EC2 : DescribeVpcs
- EC2 : DeleteNetworkInterface
- EC2 : DescribeSubnets
- EC2 : DescribeSecurityGroups

Autorisations facultatives

Votre fonction d'événement Lambda peut également avoir besoin d'autorisations pour :

- Accédez à des clusters Amazon MSK multicomptes. Pour les mappages de sources d'événements entre comptes, vous avez besoin de kafka : DescribeVpcConnection dans le rôle d'exécution. Un directeur IAM qui crée un mappage de sources d'événements entre comptes a besoin de Kafka :. ListVpcConnections

- Accédez à votre code secret SCRAM si vous utilisez l'SASL/SCRAM authentification. Ainsi, votre fonction peut utiliser un nom d'utilisateur et un mot de passe pour se connecter à Kafka.
- Décrivez le secret de votre Secrets Manager, si vous utilisez l' SASL/SCRAM authentification mTLS. Avec cette autorisation, votre fonction peut récupérer les informations d'identification ou les certificats nécessaires pour des connexions sécurisées.
- Accédez à votre clé gérée par le AWS KMS client, si votre AWS Secrets Manager secret est chiffré à l'aide d'une clé gérée par le AWS KMS client.
- Accédez aux secrets de votre registre de schémas, si vous utilisez un registre de schémas avec authentification :
  - Pour le registre des AWS Glue schémas : les besoins `glue:GetRegistry` et `glue:GetSchemaVersion` les autorisations de votre fonction. Elles permettent à votre fonction de rechercher et d'utiliser les règles de format de message stockées dans AWS Glue.
  - Pour le registre de schémas Confluent avec `BASIC_AUTH` ou `CLIENT_CERTIFICATE_TLS_AUTH` : votre fonction a besoin de l'autorisation `secretsmanager:GetSecretValue` pour accéder au secret contenant les informations d'authentification. Cela permet à votre fonction de récupérer les username/password certificats nécessaires pour accéder au registre des schémas Confluent.
  - Pour les certificats CA privés : votre fonction a besoin de l'GetSecretValue autorisation secretsmanager : pour le secret contenant le certificat. Avec cette autorisation, votre fonction peut vérifier l'identité des registres de schémas qui utilisent des certificats personnalisés.
- Accédez aux groupes de consommateurs du cluster Kafka et interrogez les messages depuis le sujet, si vous utilisez l'authentification IAM pour le mappage des sources d'événements.

Cela correspond aux autorisations requises suivantes :

- kafka : ListScramSecrets - Permet de répertorier les secrets SCRAM pour l'authentification Kafka
- secretsmanager : GetSecretValue - Permet de récupérer des secrets depuis Secrets Manager
- KMS:Decrypt - Permet le déchiffrement de données cryptées en utilisant AWS KMS
- glue : GetRegistry - Autorise l'accès au registre des AWS Glue schémas
- glue : GetSchemaVersion - Permet de récupérer des versions de schéma spécifiques à partir du registre des AWS Glue schémas
- Kafka-Cluster:connect - Accorde l'autorisation de se connecter et de s'authentifier auprès du cluster
- kafka-cluster : AlterGroup - Accorde l'autorisation de rejoindre des groupes sur un cluster, équivalent à l'ACL READ GROUP d'Apache Kafka

- kafka-cluster : DescribeGroup - Accorde l'autorisation de décrire les groupes d'un cluster, équivalent à l'ACL DESCRIBE GROUP d'Apache Kafka
- kafka-cluster : DescribeTopic - Accorde l'autorisation de décrire les sujets d'un cluster, équivalent à l'ACL DESCRIBE TOPIC d'Apache Kafka
- kafka-cluster : ReadData - Accorde l'autorisation de lire les données des rubriques d'un cluster, équivalent à l'ACL READ TOPIC d'Apache Kafka

En outre, si vous souhaitez envoyer des enregistrements d'invocations ayant échoué vers une destination en cas d'échec, vous devez disposer des autorisations suivantes en fonction du type de destination :

- Pour les destinations Amazon SQS : sqs : SendMessage - Permet d'envoyer des messages à une file d'attente Amazon SQS
- Pour les destinations Amazon SNS : sns:Publish : permet de publier des messages sur une rubrique Amazon SNS
- Pour les destinations du compartiment Amazon S3 : s3 : PutObject et s3 : ListBucket - Permet d'écrire et de répertorier des objets dans un compartiment Amazon S3

Pour résoudre les erreurs d'authentification et d'autorisation, consultez the section called "Résolution des problèmes".

Configuration de source d'événements Amazon MSK pour Lambda

Pour utiliser un cluster Amazon MSK comme source d'événements pour votre fonction d'événement Lambda, vous devez créer un mappage de source d'événements qui connecte les deux ressources. Cette page explique comment créer un mappage des sources d'événements pour Amazon MSK.

Cette page suppose que vous avez déjà correctement configuré votre cluster MSK et l'instance Amazon Virtual Private Cloud (VPC) dans lequel il réside. Si vous devez configurer votre cluster ou VPC, consultez the section called "Configuration du cluster et du réseau". Pour configurer le comportement des nouvelles tentatives afin de gérer les erreurs, consultezthe section called "Réessayer les configurations".

Rubriques

- Utilisation d'un cluster Amazon MSK en tant que source d'événement
- Configuration des méthodes d'authentification du cluster Amazon MSK dans Lambda

- Création d’un mappage des sources d’événements Lambda pour une source d’événements Amazon MSK
- Création de mappages de sources d’événements entre comptes dans Lambda
- Tous les paramètres de configuration des sources d’événements Amazon MSK dans Lambda

Utilisation d’un cluster Amazon MSK en tant que source d’événement

Lorsque vous ajoutez votre cluster Apache Kafka ou Amazon MSK comme déclencheur pour votre fonction d'événement Lambda, le cluster est utilisé comme source d'événements.

Lambda lit les données d'événements des rubriques Kafka que vous spécifiez `Topics` dans une CreateEventSourceMappingdemande, en fonction de la position de départ que vous spécifiez. Lorsque le traitement a réussi, votre rubrique Kafka est validée dans votre cluster Kafka.

Lambda lit les messages séquentiellement pour chaque partition de rubrique Kafka. Une seule charge utile Lambda peut contenir des messages provenant de plusieurs partitions. Lorsque d'autres enregistrements sont disponibles, Lambda continue de traiter les enregistrements par lots, en fonction de la BatchSize valeur que vous spécifiez dans une CreateEventSourceMappingdemande, jusqu'à ce que votre fonction aborde le sujet.

Après avoir traité chaque lot, Lambda valide les décalages des messages dans celui-ci. Si votre fonction renvoie une erreur pour l’un des messages d’un lot, Lambda réessaie le lot de messages complet jusqu’à ce que le traitement réussisse ou que les messages expirent. Vous pouvez envoyer les enregistrements qui échouent à toutes les tentatives vers une destination en cas de panne pour un traitement ultérieur.

> **Note**
>
> Alors que les fonctions d'événement Lambda ont généralement un délai d'expiration maximal de 15 minutes, les mappages de sources d'événements pour Amazon MSK, Apache Kafka autogéré, Amazon DocumentDB et Amazon MQ pour ActiveMQ et RabbitMQ ne prennent en charge que les fonctions dont le délai d'expiration maximal est de 14 minutes.

Configuration des méthodes d'authentification du cluster Amazon MSK dans Lambda

Lambda doit être autorisé à accéder à votre cluster Amazon MSK, à récupérer des enregistrements et à effectuer d’autres tâches. Amazon MSK prend en charge plusieurs méthodes d’authentification auprès de votre cluster MSK.

Méthodes d'authentification des clusters

- Accès non authentifié
- SASL/SCRAM authentication
- Authentification TLS mutuelle
- Authentification IAM
- Comment Lambda choisit un courtier bootstrap

Accès non authentifié

Si aucun client n'accède au cluster via Internet, vous pouvez utiliser un accès non authentifié.

SASL/SCRAM authentication

Lambda prend en charge l'authentification simple et l'authentification par le mécanisme d'authentification par réponse aux Layer/Salted défis de sécurité (SASL/SCRAM), avec la fonction de SHA-512 hachage et le chiffrement TLS (Transport Layer Security). Pour que Lambda se connecte au cluster, stockez les informations d'identification d'authentification (nom d'utilisateur et mot de passe) dans un secret Secrets Manager, et référencez ce secret lors de la configuration de votre mappage des sources d'événements.

Pour plus d'informations sur l'utilisation de Secrets Manager, consultez la section Authentification des Sign-in informations d'identification avec Secrets Manager dans le guide du développeur Amazon Managed Streaming for Apache Kafka.

> **Note**
>
> Amazon MSK ne prend pas en charge SASL/PLAIN l'authentification.

Authentification TLS mutuelle

Mutual TLS (mTLS) fournit une authentification bidirectionnelle entre le client et le serveur. Le client envoie un certificat au serveur pour que ce dernier vérifie le client. Le serveur envoie également un certificat au client pour que ce dernier vérifie le serveur.

Pour les intégrations Amazon MSK avec Lambda, votre cluster MSK agit en tant que serveur et Lambda en tant que client.

- Pour que Lambda puisse vérifier votre cluster MSK, vous devez configurer un certificat client en tant que secret dans Secrets Manager et référencer ce certificat dans votre configuration de mappage des sources d'événements. Le certificat client doit être signé par une autorité de certification (CA) située dans le magasin d'approbations du serveur.
- Le cluster MSK envoie également un certificat de serveur à Lambda. Le certificat du serveur doit être signé par une autorité de certification (CA) dans le AWS trust store.

Amazon MSK ne prend pas en charge les certificats de serveur autosignés. Tous les agents Amazon MSK utilisent des certificats publics signés par des autorités de certification Amazon Trust Services, auxquelles Lambda fait confiance par défaut.

Configuration du secret mTLS

Le secret CLIENT_CERTIFICATE_TLS_AUTH nécessite un champ de certificat et un champ de clé privée. Pour une clé privée chiffrée, le secret nécessite un mot de passe de clé privée. Le certificat et la clé privée doivent être au format PEM.

> **Note**
>
> Lambda prend en charge les algorithmes de chiffrement de clés privées PBES1 (mais pas PBES2).

Le champ de certificat doit contenir une liste de certificats, commençant par le certificat client, suivi de tous les certificats intermédiaires et se terminant par le certificat racine. Chaque certificat doit commencer sur une nouvelle ligne avec la structure suivante :

```
-----BEGIN CERTIFICATE-----
        <certificate contents>
-----END CERTIFICATE-----
```

Secrets Manager prend en charge les secrets jusqu'à 65 536 octets, ce qui offre suffisamment d'espace pour de longues chaînes de certificats.

La clé privée doit être au format PKCS #8, avec la structure suivante :

```
-----BEGIN PRIVATE KEY-----
         <private key contents>
-----END PRIVATE KEY-----
```

Pour une clé privée chiffrée, utilisez la structure suivante :

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
          <private key contents>
-----END ENCRYPTED PRIVATE KEY-----
```

L'exemple suivant affiche le contenu d'un secret pour l'authentification mTLS à l'aide d'une clé privée chiffrée. Pour une clé privée chiffrée, vous devez inclure le mot de passe de clé privée dans le secret.

```
{
 "privateKeyPassword": "testpassword",
 "certificate": "-----BEGIN CERTIFICATE-----
MIIE5DCCAsygAwIBAgIRAPJdwaFaNRrytHBto0j5BA0wDQYJKoZIhvcNAQELBQAw
...
j0Lh4/+1HfgyE2KlmII36dg4IMzNjAFEBZiCRoPimO40s1cRqtFHXoal0QQbIlxk
cmUuiAii9R0=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIFgjCCA2qgAwIBAgIQdjNZd6uFf9hbNC5RdfmHrzANBgkqhkiG9w0BAQsFADBb
...
rQoiowbbk5wXCheYSANQIfTZ6weQTgiCHCCbuuMKNVS95FkXm0vqVD/YpXKwA/no
c8PH3PSoAaRwMMgOSA2ALJvbRz8mpg==
-----END CERTIFICATE-----",
 "privateKey": "-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFKzBVBgkqhkiG9w0BBQ0wSDAnBgkqhkiG9w0BBQwwGgQUiAFcK5hT/X7Kjmgp
...
QrSekqF+kWzmB6nAfSzgO9IaoAaytLvNgGTckWeUkWn/V0Ck+LdGUXzAC4RxZnoQ
zp2mwJn2NYB7AZ7+imp0azDZb+8YG2aUCiyqb6PnnA==
-----END ENCRYPTED PRIVATE KEY-----"
}
```

Pour plus d'informations sur le protocole mTLS pour Amazon MSK et des instructions sur la génération d'un certificat client, consultez Authentification de client TLS mutuel pour Amazon MSK dans le Guide du développeur Amazon Managed Streaming for Apache Kafka.

Authentification IAM

Vous pouvez utiliser Gestion des identités et des accès AWS (IAM) pour authentifier l'identité des clients qui se connectent au cluster MSK. Avec l'authentification IAM, Lambda s'appuie sur les autorisations associées au rôle d'exécution de votre fonction d'événement pour se connecter au cluster, récupérer des enregistrements et effectuer d'autres actions requises. Pour un exemple de

politique contenant les autorisations nécessaires, consultez Créer des politiques d'autorisation pour le rôle IAM dans le Guide du développeur Amazon Managed Streaming pour Apache Kafka.

Si l'authentification IAM est active sur votre cluster MSK et que vous ne fournissez pas de secret, Lambda utilise automatiquement l'authentification IAM par défaut.

Pour de plus amples informations sur l'authentification IAM dans Amazon MSK, veuillez consulter Contrôle d'accès IAM.

Comment Lambda choisit un courtier bootstrap

Lambda choisit un courtier d'amorçage en fonction des méthodes d'authentification disponibles sur votre cluster, et si vous fournissez un secret pour l'authentification. Si vous fournissez un secret pour MTL ou SASL/SCRAM, Lambda choisit automatiquement cette méthode d'authentification. Si vous ne e faites pas, Lambda sélectionne la méthode d'authentification la plus puissante active sur votre cluster. Voici l'ordre de priorité dans lequel Lambda sélectionne un courtier, de l'autorisation la plus forte à la plus faible :

- MTLs (secret fourni pour les mTLS)
- SASL/SCRAM (secret prévu SASL/SCRAM)
- SASL IAM (aucun secret fourni et authentification IAM active)
- TLS non authentifié (aucun secret fourni et authentification IAM non active)
- Texte brut (aucun secret n'est fourni, et l'authentification IAM et le TLS non authentifié ne sont pas actifs)

> **Note**
>
> Si Lambda ne parvient pas à se connecter au type de courtier le plus sécurisé, Lambda n'essaie pas de se connecter à un type de courtier différent (plus faible). Si vous souhaitez que Lambda choisisse un type de courtier plus faible, désactivez toutes les méthodes d'authentification plus puissantes sur votre cluster.

Création d'un mappage des sources d'événements Lambda pour une source d'événements Amazon MSK

Pour créer un mappage des sources d'événements, vous pouvez utiliser la console Lambda, AWS Command Line Interface (CLI) ou un SDK AWS.

> **Note**
>
> Lorsque vous créez le mappage des sources d'événements, Lambda crée une ENI Hyperplane dans le sous-réseau privé qui contient votre cluster MSK, ce qui permet à Lambda d'établir une connexion sécurisée. Cet hyperplan autorisé par l'ENI utilise la configuration du sous-réseau et du groupe de sécurité de votre cluster MSK, et non votre fonction d'événement Lambda.

Les étapes de console suivantes ajoutent un cluster Amazon MSK comme déclencheur pour votre fonction d'événement Lambda. En arrière-plan, cela crée une ressource de mappage des sources d'événements.

Pour ajouter un déclencheur Amazon MSK à votre fonction d'événement Lambda (console)

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez le nom de la fonction d'événement Lambda à laquelle vous souhaitez ajouter un déclencheur Amazon MSK.
3. Sous Function overview (Vue d'ensemble de la fonction), choisissez Add trigger (Ajouter un déclencheur).
4. Sous Trigger configuration (Configuration du déclencheur), choisissez MSK.
5. Pour spécifier les détails de votre cluster Kafka, procédez comme suit :
    1. Pour MSK cluster (Cluster MSK), sélectionnez votre cluster.
    2. Dans Nom de la rubrique, donnez un nom à la rubrique Kafka dont vous souhaitez consommer les messages.
    3. Pour l'identifiant de groupe de consommateurs, entrez l'identifiant d'un groupe de consommateurs Kafka à rejoindre, le cas échéant. Pour plus d'informations, consultez the section called "ID de groupe de consommateurs".
6. Pour Authentification du cluster, effectuez les configurations nécessaires. Pour plus d'informations sur l'authentification du cluster, consultez the section called "Authentification du cluster".
    - Activez Utiliser l'authentification si vous souhaitez que Lambda effectue l'authentification auprès de votre cluster MSK lors de l'établissement d'une connexion. L'authentification est recommandée.

- Si vous utilisez l'authentification, dans Méthode d'authentification, choisissez la méthode d'authentification à utiliser.
- Si vous utilisez l'authentification, pour Clé Secrets Manager, choisissez la clé Secrets Manager qui contient les informations d'identification d'authentification nécessaires pour accéder à votre cluster.

7. Sous Configuration des sondeurs d'événements, effectuez les configurations nécessaires.

   - Choisissez Activer le déclencheur pour activer le déclencheur immédiatement après sa création.
   - Choisissez si vous souhaitez Configurer le mode provisionné pour votre mappage des sources d'événements. Pour plus d'informations, consultez the section called "Mise à l'échelle des sondeurs d'événements".
     - Si vous configurez le mode provisionné, entrez une valeur pour Minimum Event Sollers, une valeur pour Maximum Event Sollers et une valeur facultative PollerGroupName pour spécifier le regroupement de plusieurs ESM au sein du même VPC source d'événements.
   - Dans Position de départ, choisissez la façon dont vous souhaitez que Lambda commence à lire à partir de votre flux. Pour plus d'informations, consultez the section called "Positions des interrogations et des flux".

8. Sous Traitement par lots, effectuez les configurations nécessaires. Pour plus d'informations sur la mise en lots, consultez the section called "Comportement de traitement par lots".

   1. Pour Batch size (Taille de lot), entrez le nombre maximum d'enregistrements à recevoir dans un même lot.
   2. Pour Batch window, veuillez saisir le nombre maximal de secondes nécessaires à Lambda pour collecter des enregistrements avant d'invoquer la fonction.

9. Sous Filtrage, effectuez les configurations nécessaires. Pour plus d'informations sur le filtrage, veuillez consulter la rubrique the section called "Filtrage des événements".

   - Pour Critères de filtre, ajoutez des définitions de critères de filtre pour déterminer s'il faut ou non traiter un événement.

10. Sous Gestion des échecs, effectuez les configurations nécessaires. Pour plus d'informations sur la gestion des échecs, consultez the section called "Conserver les appels ayant échoué".

    - Pour la On-failure destination, spécifiez l'ARN de votre destination en cas de défaillance.

11. Pour Balises, saisissez les balises à associer à ce mappage des sources d'événements.

12. Pour créer le déclencheur, choisissez Add (Ajouter).

Vous pouvez également créer le mappage des sources d'événements à l'aide de la AWS CLI avec la commande create-event-source-mapping. L'exemple suivant crée un mappage de source d'événements pour associer la fonction d'événement Lambda `my-msk-function` au `AWSKafkaTopic` sujet, en commençant par le `LATEST` message. Cette commande utilise également l'SourceAccessConfigurationobjet pour demander à Lambda d'SASL/SCRAMutiliser l'authentification lors de la connexion au cluster.

```
aws lambda create-event-source-mapping \
  --event-source-arn arn:aws:kafka:us-east-1:111122223333:cluster/my-cluster/fc2f5bdf-
fd1b-45ad-85dd-15b4a5a6247e-2 \
  --topics AWSKafkaTopic \
  --starting-position LATEST \
  --function-name my-kafka-function
  --source-access-configurations '[{"Type": "SASL_SCRAM_512_AUTH","URI":
 "arn:aws:secretsmanager:us-east-1:111122223333:secret:my-secret"}]'
```

Si le cluster utilise l'authentification mTLS, incluez un SourceAccessConfigurationobjet qui le spécifie `CLIENT_CERTIFICATE_TLS_AUTH` et un ARN de clé Secrets Manager. En voici un exemple dans la commande suivante :

```
aws lambda create-event-source-mapping \
  --event-source-arn arn:aws:kafka:us-east-1:111122223333:cluster/my-cluster/fc2f5bdf-
fd1b-45ad-85dd-15b4a5a6247e-2 \
  --topics AWSKafkaTopic \
  --starting-position LATEST \
  --function-name my-kafka-function
  --source-access-configurations '[{"Type": "CLIENT_CERTIFICATE_TLS_AUTH","URI":
 "arn:aws:secretsmanager:us-east-1:111122223333:secret:my-secret"}]'
```

Lorsque le cluster utilise l'authentification IAM, vous n'avez pas besoin d' SourceAccessConfigurationobjet. En voici un exemple dans la commande suivante :

```
aws lambda create-event-source-mapping \
  --event-source-arn arn:aws:kafka:us-east-1:111122223333:cluster/my-cluster/fc2f5bdf-
fd1b-45ad-85dd-15b4a5a6247e-2 \
  --topics AWSKafkaTopic \
  --starting-position LATEST \
  --function-name my-kafka-function
```

Création de mappages de sources d’événements entre comptes dans Lambda

Vous pouvez utiliser la connectivité privée multi-VPC pour connecter une fonction d'événement Lambda à un cluster MSK provisionné dans un autre. Compte AWS Multi-VPC la connectivité utilise AWS PrivateLink, ce qui permet de maintenir tout le trafic sur le AWS réseau.

> **Note**
>
> Vous ne pouvez pas créer de mappages de sources d’événements entre comptes pour les clusters MSK sans serveur.

Pour créer un mappage des sources d’événements entre comptes, vous devez d’abord configurer la connectivité multi-VPC pour le cluster MSK. Lorsque vous créez le mappage des sources d’événements, utilisez l’ARN de connexion VPC géré au lieu de l’ARN du cluster, comme indiqué dans les exemples suivants. Le CreateEventSourceMappingfonctionnement varie également en fonction du type d'authentification utilisé par le cluster MSK.

Example— Crée un mappage des sources d’événements entre comptes pour le cluster qui utilise l’authentification IAM

Lorsque le cluster utilise l'authentification basée sur les rôles IAM, vous n'avez pas besoin d'objet. SourceAccessConfiguration Exemple :

```
aws lambda create-event-source-mapping \
  --event-source-arn arn:aws:kafka:us-east-1:111122223333:vpc-connection/444455556666/
my-cluster-name/51jn98b4-0a61-46cc-b0a6-61g9a3d797d5-7 \
  --topics AWSKafkaTopic \
  --starting-position LATEST \
  --function-name my-kafka-function
```

Example— Créez un mappage des sources d'événements entre comptes pour le cluster qui utilise l'authentification SASL/SCRAM

Si le cluster utilise SASL/SCRAM l'authentification, vous devez inclure un SourceAccessConfigurationobjet qui spécifie `SASL_SCRAM_512_AUTH` et un ARN secret de Secrets Manager.

Il existe deux manières d'utiliser les secrets pour les mappages de sources d'événements Amazon MSK entre comptes avec authentification : SASL/SCRAM

- Créez un secret dans le compte Lambda Event Function et synchronisez-le avec le secret du cluster. Créez une rotation pour synchroniser les deux secrets. Cette option vous permet de contrôler le secret du compte de fonction.
- Utilisez le secret associé au cluster MSK. Ce secret doit autoriser l'accès entre comptes au compte Lambda Event Function. Pour plus d'informations, voir Autorisations d'accéder aux secrets AWS Secrets Manager pour les utilisateurs d'un autre compte.

```
aws lambda create-event-source-mapping \
  --event-source-arn arn:aws:kafka:us-east-1:111122223333:vpc-connection/444455556666/
my-cluster-name/51jn98b4-0a61-46cc-b0a6-61g9a3d797d5-7 \
  --topics AWSKafkaTopic \
  --starting-position LATEST \
  --function-name my-kafka-function \
  --source-access-configurations '[{"Type": "SASL_SCRAM_512_AUTH","URI":
 "arn:aws:secretsmanager:us-east-1:444455556666:secret:my-secret"}]'
```

Example— Crée un mappage des sources d'événements entre comptes pour le cluster qui utilise l'authentification mTLS

Si le cluster utilise l'authentification mTLS, vous devez inclure un SourceAccessConfigurationobjet qui spécifie `CLIENT_CERTIFICATE_TLS_AUTH` et un ARN secret de Secrets Manager. Le secret peut être stocké dans le compte du cluster ou dans le compte Lambda Event Function.

```
aws lambda create-event-source-mapping \
  --event-source-arn arn:aws:kafka:us-east-1:111122223333:vpc-connection/444455556666/
my-cluster-name/51jn98b4-0a61-46cc-b0a6-61g9a3d797d5-7 \
  --topics AWSKafkaTopic \
  --starting-position LATEST \
  --function-name my-kafka-function \
  --source-access-configurations '[{"Type": "CLIENT_CERTIFICATE_TLS_AUTH","URI":
 "arn:aws:secretsmanager:us-east-1:444455556666:secret:my-secret"}]'
```

Tous les paramètres de configuration des sources d'événements Amazon MSK dans Lambda

Tous les types de sources d'événements Lambda partagent les mêmes opérations CreateEventSourceMappinget les mêmes opérations d'UpdateEventSourceMappingAPI. Cependant, seuls certains paramètres s'appliquent à Amazon MSK, comme indiqué dans le tableau suivant.

Paramètre	Obligatoire	Par défaut	Remarques
AmazonManagedKafkaEventSourceConfig	N	Contient le ConsumerGroupId champ, dont la valeur par défaut est unique.	Peut définir uniquement sur Create (Créer)
BatchSize	N	100	Maximum : 10 000.
DestinationConfig	N	N/A	the section called “Conserver les appels ayant échoué”
Activé	N	True	
BisectBatchOnFunctionError	N	False	the section called “Réessayer les configurations”
FunctionResponseTypes	N	N/A	the section called “Réessayer les configurations”
MaximumRecordAgeInSeconds	N	-1 (infini)	the section called “Réessayer les configurations”
MaximumRetryAttempts	N	-1 (infini)	the section called “Réessayer les configurations”
EventSourceArn	O	N/A	Peut définir uniquement sur Create (Créer)
FilterCriteria	N	N/A	Contrôlez les événements que Lambda envoie

Paramètre	Obligatoire	Par défaut	Remarques
			à votre fonction d'événement
FunctionName	O	N/A	
KMSKeyArn	N	N/A	the section called “Chiffrement des critères de filtre”
MaximumBatchingWindowInSeconds	N	500 ms	Comportement de traitement par lots
ProvisionedPollersConfig	N	`MinimumPollers` : la valeur par défaut, si elle n’est pas spécifiée, est de 1 `MaximumPollers` : la valeur par défaut, si elle n’est pas spécifiée, est de 200 `PollerGroupName` : N/A	the section called “Mode alloué”
SourceAccessConfigurations	N	Pas d’informations d’identification	SASL/SCRAM ou identifiants d'authentification CLIENT_CERTIFICATE_TLS_AUTH (MutualTLS) pour votre source d'événement

Paramètre	Obligatoire	Par défaut	Remarques
StartingPosition	O	N/A	AT_TIMESTAMP, TRIM_HORIZON ou DERNIER Peut définir uniquement sur Create (Créer)
StartingPositionTimestamp	N	N/A	Obligatoire s'il StartingPosition est défini sur AT_TIMESTAMP
Étiquettes	N	N/A	the section called “Balises de mappage des sources d’événements”
Rubriques	O	N/A	Nom de rubrique Kafka Peut définir uniquement sur Create (Créer)

Note

Lorsque vous spécifiez un`PollerGroupName`, plusieurs ESM au sein d'un même Amazon VPC peuvent partager la capacité de l'Event Poller Unit (EPU). Vous pouvez utiliser cette option pour optimiser les coûts du mode provisionné pour vos ESM. Exigences relatives au regroupement ESM :

- Les ESM doivent se trouver au sein du même Amazon VPC
- Maximum de 100 ESM par groupe de sondeurs

- Le nombre maximum de sondeurs agrégés pour tous les ESM d'un groupe ne peut pas dépasser 2 000

Vous pouvez le mettre `PollerGroupName` à jour pour déplacer un ESM vers un autre groupe, ou supprimer un ESM d'un groupe en le définissant `PollerGroupName` sur une chaîne vide (« »).

Tutoriel : Utilisation d'un mappage de source d'événements Amazon MSK pour appeler une fonction d'événement Lambda

Dans ce didacticiel, vous allez effectuer les opérations suivantes :

- Créez une fonction d'événement Lambda dans le même AWS compte qu'un cluster Amazon MSK existant.
- Configurer le réseau et l’authentification pour que Lambda communique avec Amazon MSK.
- Configurez un mappage des sources d'événements Lambda Amazon MSK, qui exécute votre fonction lorsque des événements apparaissent dans la rubrique.

Une fois ces étapes terminées, lorsque des événements sont envoyés à Amazon MSK, vous pouvez configurer une fonction pour traiter ces événements automatiquement avec votre propre code Lambda personnalisé.

Que pouvez-vous faire avec cette fonctionnalité ?

Exemple de solution : Utiliser un mappage des sources d’événements MSK pour fournir des résultats en direct à vos clients.

Imaginons le scénario suivant : votre entreprise héberge une application Web dans laquelle vos clients peuvent consulter des informations sur des événements en direct, tels que des matchs de sport. Les informations actualisées du jeu sont fournies à votre équipe via une rubrique Kafka sur Amazon MSK. Vous souhaitez concevoir une solution qui utilise les mises à jour issues de la rubrique MSK afin de fournir une vue actualisée de l’événement en direct aux clients au sein d’une application que vous développez. Vous avez opté pour l'approche de conception suivante : Vos applications clientes communiquent avec un backend sans serveur hébergé dans. AWS Les clients se connectent via des sessions Websocket à l'aide de l'API Amazon WebSocket API Gateway.

Dans cette solution, vous avez besoin d'un composant qui lit les événements MSK, exécute une logique personnalisée pour préparer ces événements pour la couche application, puis transmet ces informations à l'API API Gateway. Vous pouvez implémenter ce composant en fournissant votre logique personnalisée dans une fonction, puis en l'appelant à l'aide d'un mappage de source d'événements AWS Lambda Amazon MSK. AWS Lambda

Pour plus d'informations sur la mise en œuvre de solutions à l'aide de l'API Amazon WebSocket API Gateway, consultez les WebSocket didacticiels sur les API dans la documentation d'API Gateway.

Conditions préalables

Un AWS compte avec les ressources préconfigurées suivantes :

Pour remplir ces prérequis, nous vous recommandons de suivre Get started using Amazon MSK dans la documentation Amazon MSK.

- Un cluster Amazon MSK. Consultez Create an Amazon MSK cluster dans Getting started using Amazon MSK.
- La configuration suivante :
  - Assurez-vous que l'authentification basée sur les rôles IAM est Activée dans les paramètres de sécurité de votre cluster. Cela améliore votre sécurité en limitant votre fonction d'événement Lambda à l'accès uniquement aux ressources Amazon MSK nécessaires. L'authentification basée sur les rôles IAM est activée par défaut sur les nouveaux clusters Amazon MSK.
  - Assurez-vous que l'Accès public est désactivé dans les paramètres réseau de votre cluster. Restreindre l'accès à Internet de votre cluster Amazon MSK améliore votre sécurité en limitant le nombre d'intermédiaires qui traitent vos données. L'accès public est activé par défaut sur les nouveaux clusters Amazon MSK.
- Une rubrique Kafka dans votre cluster Amazon MSK à utiliser pour cette solution. Consultez Create a topic dans Getting started using Amazon MSK.
- Un hôte administrateur Kafka configuré pour extraire les informations de votre cluster Kafka et envoyer des événements Kafka à votre rubrique à des fins de test, par exemple une instance Amazon EC2 sur laquelle la CLI d'administration Kafka et la bibliothèque IAM Amazon MSK sont installées. Consultez Create a client machine dans Getting started using Amazon MSK.

Une fois que vous avez configuré ces ressources, collectez les informations suivantes à partir de votre AWS compte pour confirmer que vous êtes prêt à continuer.

- Le nom de votre cluster Amazon MSK. Vous pouvez trouver cette information dans la console Amazon MSK.
- L'UUID du cluster, qui fait partie de l'ARN de votre cluster Amazon MSK, que vous pouvez trouver dans la console Amazon MSK. Suivez les procédures décrites dans la rubrique Listing clusters de la documentation Amazon MSK pour trouver cette information.
- Les groupes de sécurité associés à votre cluster Amazon MSK. Vous pouvez trouver cette information dans la console Amazon MSK. Dans les étapes suivantes, appelez-les vos*clusterSecurityGroups*.
- L'ID du VPC Amazon contenant votre cluster Amazon MSK. Vous pouvez trouver cette information en identifiant les sous-réseaux associés à votre cluster Amazon MSK dans la console Amazon MSK, puis en identifiant le VPC Amazon associé au sous-réseau dans la console Amazon VPC.
- Le nom de la rubrique Kafka utilisée dans votre solution. Vous pouvez trouver cette information en appelant votre cluster Amazon MSK à l'aide de la CLI `topics` Kafka depuis votre hôte administrateur Kafka. Pour plus d'informations sur la CLI de rubriques, consultez la section Adding and removing topics dans la documentation Kafka.
- Le nom d'un groupe de consommateurs pour votre sujet Kafka, adapté à une utilisation par votre fonction d'événement Lambda. Ce groupe peut être créé automatiquement par Lambda. Vous n'avez donc pas besoin de le créer avec la CLI Kafka. Si vous devez gérer vos groupes de consommateurs, pour en savoir plus sur la CLI de groupes de consommateurs, consultez la rubrique Managing Consumer Groups dans la documentation Kafka.

Les autorisations suivantes dans votre AWS compte :

- Autorisation de créer et de gérer une fonction.
- Autorisation de créer des politiques IAM et de les associer à votre fonction.
- L'autorisation de créer des points de terminaison de VPC Amazon et de modifier la configuration réseau dans le VPC Amazon hébergeant votre cluster Amazon MSK.

Installer la AWS Command Line Interface

Si vous ne l'avez pas encore installé AWS Command Line Interface, suivez les étapes décrites dans la section Installation ou mise à jour de la dernière version du AWS CLI pour l'installer.

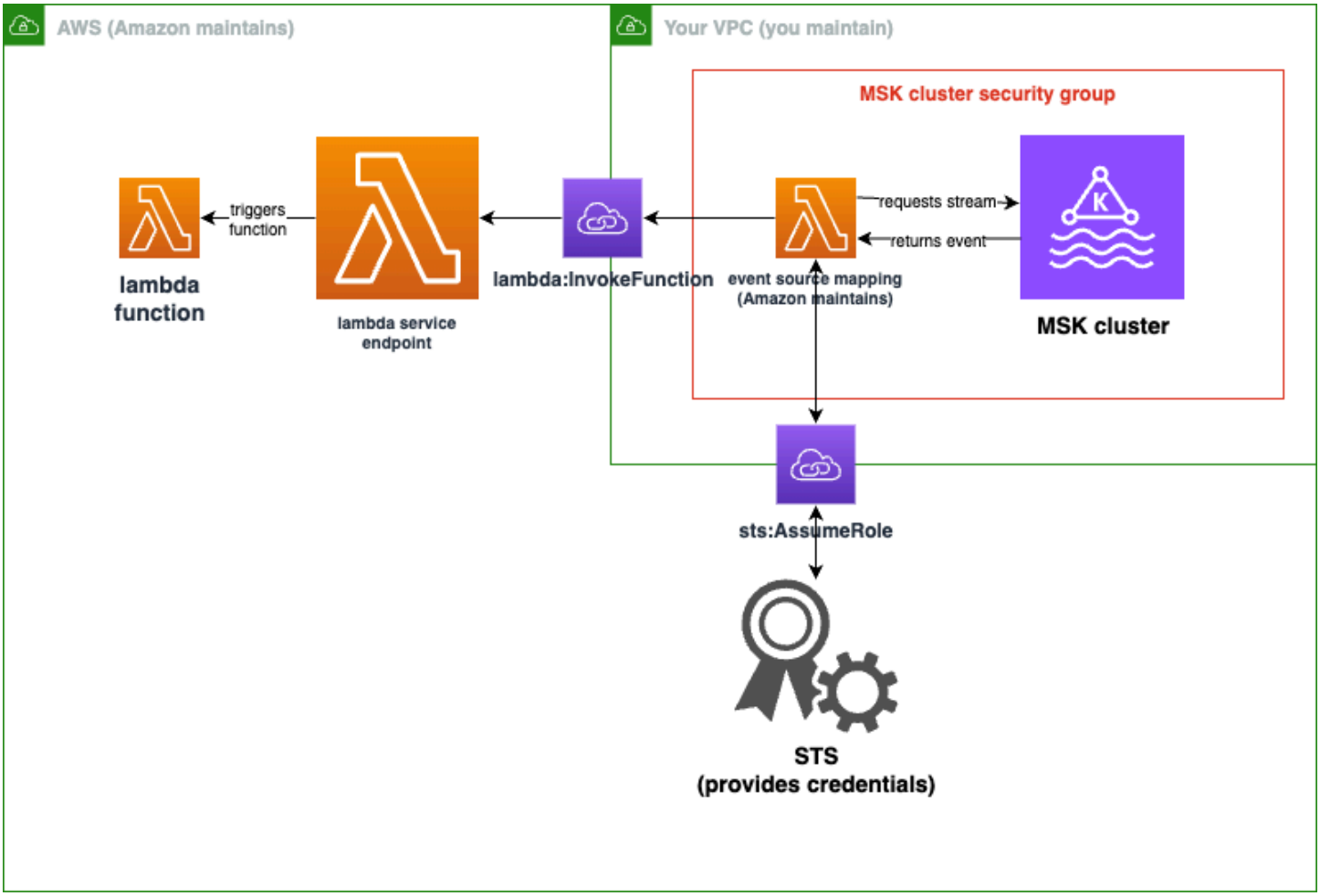
Ce tutoriel nécessite un terminal de ligne de commande ou un shell pour exécuter les commandes. Sous Linux et macOS, utilisez votre gestionnaire de shell et de package préféré.

> **Note**
>
> Sous Windows, certaines commandes CLI Bash que vous utilisez couramment avec Lambda (par exemple `zip`) ne sont pas prises en charge par les terminaux intégrés du système d'exploitation. Pour obtenir une Windows-integrated version d'Ubuntu et de Bash, installez le sous-système Windows pour Linux.

Configurer la connectivité réseau pour que Lambda communique avec Amazon MSK

AWS PrivateLink À utiliser pour connecter Lambda et Amazon MSK. Pour ce faire, vous créez des points de terminaison de VPC Amazon d'interface dans la console Amazon VPC. Pour plus d'informations sur la configuration réseau, consultez the section called "Configuration du cluster et du réseau".

Lorsqu'un mappage de source d'événement Amazon MSK s'exécute pour le compte d'une fonction d'événement Lambda, il assume le rôle d'exécution de la fonction. Ce rôle IAM autorise le mappage pour accéder aux ressources sécurisées par IAM, telles que votre cluster Amazon MSK. Bien que les composants partagent un rôle d'exécution, le mappage Amazon MSK et votre fonction ont des exigences de connectivité distinctes pour leurs tâches respectives, comme le montre le schéma suivant.



Votre mappage des sources d'événements appartient au groupe de sécurité de votre cluster Amazon MSK. Au cours de cette étape de mise en réseau, créez des points de terminaison de VPC Amazon à partir de votre VPC de cluster Amazon MSK pour connecter le mappage des sources d'événements aux services Lambda et STS. Sécurisez ces points de terminaison pour accepter le trafic provenant du groupe de sécurité de votre cluster Amazon MSK. Ajustez ensuite les groupes de sécurité du cluster Amazon MSK pour permettre au mappage des sources d'événements de communiquer avec le cluster Amazon MSK.

Vous pouvez configurer les étapes suivantes à l'aide de l' Console de gestion AWS.

Pour configurer les points de terminaison de VPC Amazon d'interface afin de connecter Lambda et Amazon MSK

1. Créez un groupe de sécurité pour les points de terminaison Amazon VPC de votre interface*endpointSecurityGroup*, qui autorise le trafic TCP entrant sur 443 depuis. *clusterSecurityGroups* Suivez la procédure décrite dans la rubrique Create a security

group de la documentation Amazon EC2 pour créer un groupe de sécurité. Suivez ensuite la procédure décrite dans la rubrique Add rules to a security group de la documentation Amazon EC2 pour ajouter les règles appropriées.

Créez un groupe de sécurité avec les informations suivantes :

Lorsque vous ajoutez vos règles de trafic entrant, créez une règle pour chaque groupe de sécurité dans*clusterSecurityGroups*. Pour chaque règle :

- Dans le champ Type, sélectionnez HTTPS.
- Pour Source, sélectionnez l'un des*clusterSecurityGroups*.

2. Créez un point de terminaison connectant le service Lambda au VPC Amazon qui contient votre cluster Amazon MSK. Suivez la procédure décrite dans Create an interface endpoint.

   Créez un point de terminaison d'interface avec les informations suivantes :

   - Dans Nom du service`com.amazonaws.`*regionName*`.lambda`, sélectionnez où *regionName* héberge votre fonction.
   - Pour VPC, sélectionnez le VPC Amazon contenant votre cluster Amazon MSK.
   - Pour les groupes de sécurité*endpointSecurityGroup*, sélectionnez ceux que vous avez créés précédemment.
   - Pour Sous-réseaux, sélectionnez les sous-réseaux qui hébergent votre cluster Amazon MSK.
   - Pour Politique, fournissez le document de politique suivant, qui sécurise le point de terminaison afin qu'il soit utilisé par le principal de service Lambda pour l'action `lambda:InvokeFunction`.

```
{
    "Statement": [
        {
            "Action": "lambda:InvokeFunction",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "lambda.amazonaws.com"
                ]
            },
            "Resource": "*"
        }
    ]
```

```
}
```

- Assurez-vous que Activer le nom DNS reste défini.

3. Créez un point de terminaison connectant le AWS STS service au Amazon VPC contenant votre cluster Amazon MSK. Suivez la procédure décrite dans Create an interface endpoint.

   Créez un point de terminaison d'interface avec les informations suivantes :

   - Pour Nom du service, sélectionnez AWS STS.
   - Pour VPC, sélectionnez le VPC Amazon contenant votre cluster Amazon MSK.
   - Pour les groupes de sécurité, sélectionnez*endpointSecurityGroup*.
   - Pour Sous-réseaux, sélectionnez les sous-réseaux qui hébergent votre cluster Amazon MSK.
   - Pour Politique, fournissez le document de politique suivant, qui sécurise le point de terminaison afin qu'il soit utilisé par le principal de service Lambda pour l'action `sts:AssumeRole`.

   ```
   {
       "Statement": [
           {
               "Action": "sts:AssumeRole",
               "Effect": "Allow",
               "Principal": {
                   "Service": [
                       "lambda.amazonaws.com"
                   ]
               },
               "Resource": "*"
           }
       ]
   }
   ```

   - Assurez-vous que Activer le nom DNS reste défini.

4. Pour chaque groupe de sécurité associé à votre cluster Amazon MSK, c'est-à-dire dans*clusterSecurityGroups*, autorisez ce qui suit :

   - Autorisez tout le trafic TCP entrant et sortant sur le 9098 à tous*clusterSecurityGroups*, y compris à l'intérieur de celui-ci.
   - Autorisez tout le trafic TCP sortant sur le port 443.

Une partie de ce trafic est autorisée par les règles des groupes de sécurité par défaut. Par conséquent, si votre cluster est attaché à un seul groupe de sécurité et que ce groupe possède des règles par défaut, il n'est pas nécessaire d'ajouter des règles. Pour ajuster les règles de groupe de sécurité, suivez les procédures décrites dans la rubrique Add rules to a security group de la documentation Amazon EC2.

Ajoutez des règles à vos groupes de sécurité avec les informations suivantes :

- Pour chaque règle entrante ou sortante pour le port 9098, indiquez
  - Pour Type, sélectionnez Custom TCP (TCP personnalisé).
  - Pour Plage de ports, indiquez 9098.
  - Pour Source, indiquez l'un des *clusterSecurityGroups*.
- Pour chaque règle entrante pour le port 443, pour Type, sélectionnez HTTPS.

Créer un rôle IAM pour que Lambda puisse lire un extrait de votre rubrique Amazon MSK

Identifiez les exigences d'authentification que Lambda doit lire dans votre rubrique Amazon MSK, puis définissez-les dans une politique. Créez un rôle qui autorise Lambda à utiliser ces autorisations. *lambdaAuthRole* Autorisez les actions sur votre cluster Amazon MSK à l'aide d'actions IAM `kafka-cluster`. Autorisez ensuite Lambda à effectuer les actions Amazon MSK et Amazon `kafka` EC2 nécessaires pour découvrir et vous connecter à votre cluster Amazon MSK, ainsi que les actions permettant à Lambda de consigner CloudWatch ce qu'il a fait.

Pour décrire les exigences d'authentification pour que Lambda puisse lire depuis Amazon MSK

1. Rédigez un document de politique IAM (un document JSON) qui permet à Lambda de lire un extrait de votre sujet Kafka dans votre cluster Amazon MSK en utilisant votre groupe de consommateurs Kafka. *clusterAuthPolicy* Lambda nécessite qu'un groupe de consommateurs Kafka soit défini lors de la lecture.

   Modifiez le modèle suivant pour l'aligner sur vos prérequis :

   JSON

```
{
    "Version":"2012-10-17",
```

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kafka-cluster:Connect",
                "kafka-cluster:DescribeGroup",
                "kafka-cluster:AlterGroup",
                "kafka-cluster:DescribeTopic",
                "kafka-cluster:ReadData",
                "kafka-cluster:DescribeClusterDynamicConfiguration"
            ],
            "Resource": [
                "arn:aws:kafka:us-
east-1:111122223333:cluster/mskClusterName/cluster-uuid",
                "arn:aws:kafka:us-
east-1:111122223333:topic/mskClusterName/cluster-uuid/mskTopicName",
                "arn:aws:kafka:us-
east-1:111122223333:group/mskClusterName/cluster-uuid/mskGroupName"
            ]
        }
    ]
}
```

Pour plus d'informations, consultez the section called "Configurer les autorisations ". Lorsque vous rédigez votre politique :

- Remplacez *us-east-1* et *111122223333* par le Région AWS et Compte AWS de votre cluster Amazon MSK.
- Pour*mskClusterName*, indiquez le nom de votre cluster Amazon MSK.
- Pour*cluster-uuid*, fournissez l'UUID dans l'ARN de votre cluster Amazon MSK.
- Pour*mskTopicName*, indiquez le nom de votre sujet Kafka.
- Pour*mskGroupName*, indiquez le nom de votre groupe de consommateurs Kafka.

2. Identifiez Amazon MSK, Amazon EC2 CloudWatch et les autorisations requises pour que Lambda découvre et connecte votre cluster Amazon MSK, puis enregistrez ces événements.

   La politique gérée `AWSLambdaMSKExecutionRole` définit de manière permissive les autorisations requises. Utilisez-la dans les étapes suivantes.

Dans un environnement de production, évaluez `AWSLambdaMSKExecutionRole` pour restreindre votre politique de rôle d'exécution sur la base du principe du moindre privilège, puis rédigez une politique pour votre rôle qui remplace cette politique gérée.

Pour plus d'informations sur le langage de politique IAM, consultez la documentation IAM.

Maintenant que vous avez rédigé votre document de politique, créez une politique IAM afin de pouvoir l'attacher à votre rôle. Pour ce faire, vous pouvez utiliser la console en suivant la procédure ci-dessous.

Pour créer une politique IAM à partir de votre document de politique

1. Connectez-vous à la console IAM Console de gestion AWS et ouvrez-la à https://console.aws.amazon.com/iam/l'adresse.
2. Dans le panneau de navigation de gauche, choisissez Politiques.
3. Choisissez Create Policy (Créer une politique).
4. Dans la section Éditeur de politiques, choisissez l'option JSON.
5. Coller*clusterAuthPolicy*.
6. Lorsque vous avez fini d'ajouter des autorisations à la politique, choisissez Suivant.
7. Sur la page Vérifier et créer, tapez un Nom de politique et une Description (facultative) pour la politique que vous créez. Vérifiez les Autorisations définies dans cette politique pour voir les autorisations accordées par votre politique.
8. Choisissez Create policy (Créer une politique) pour enregistrer votre nouvelle politique.

Pour plus d'informations, consultez Création de politiques IAM dans la documentation IAM.

Maintenant que vous disposez des politiques IAM appropriées, créez un rôle et attachez-les à celui-ci. Pour ce faire, vous pouvez utiliser la console en suivant la procédure ci-dessous.

Pour créer un rôle d'exécution dans la console IAM

1. Ouvrez la page Roles (Rôles) dans la console IAM.
2. Choisissez Créer un rôle.
3. Sous Trusted entity type (Type d'entité approuvée), choisissez service AWS .
4. Sous Cas d'utilisation, choisissez Lambda.

5. Choisissez Suivant.
6. Sélectionnez les stratégies suivantes :
   - *clusterAuthPolicy*
   - AWSLambdaMSKExecutionRole
7. Choisissez Suivant.
8. Dans Nom du rôle, entrez *lambdaAuthRole* puis choisissez Créer un rôle.

Pour plus d'informations, consultez the section called "Rôle d'exécution (autorisations pour les fonctions d'accéder à d'autres ressources)".

Créez une fonction d'événement Lambda pour lire un extrait de votre rubrique Amazon MSK

Créez une fonction d'événement Lambda configurée pour utiliser votre rôle IAM. Vous pouvez créer votre fonction à l'aide de la console.

Pour créer une fonction à l'aide de votre configuration d'authentification

1. Ouvrez la console Lambda et sélectionnez Create Event Function dans l'en-tête.
2. Sélectionnez Créer à partir de zéro.
3. Pour Nom de la fonction, saisissez un nom approprié de votre choix.
4. Pour Environnement d'exécution, choisissez la dernière version prise en charge (Dernier pris en charge) de `Node.js` pour utiliser le code fourni dans ce tutoriel.
5. Choisissez Modifier le rôle d'exécution par défaut.
6. Sélectionnez Utiliser un rôle existant.
7. Pour Rôle existant, sélectionnez*lambdaAuthRole*.

Dans un environnement de production, vous devez généralement ajouter des politiques supplémentaires au rôle d'exécution de votre fonction d'événement Lambda afin de traiter de manière significative vos événements Amazon MSK. Pour plus d'informations sur l'ajout de politiques à votre rôle, consultez la section Ajouter ou supprimer des autorisations d'identité dans la documentation IAM.

Créez une source d'événement mappée à votre fonction d'événement Lambda

Votre mappage des sources d'événements Amazon MSK fournit au service Lambda les informations nécessaires pour invoquer votre fonction Lambda lorsque des événements Amazon MSK appropriés

se produisent. Vous pouvez créer un mappage Amazon MSK à l'aide de la console. Créez un déclencheur Lambda, puis le mappage des sources d'événements est automatiquement configuré.

Pour créer un déclenceur Lambda (et un mappage des sources d'événements)

1. Accédez à la page de présentation de votre fonction d'événement Lambda.
2. Dans la section Vue d'ensemble de la fonction événementielle, choisissez Ajouter un déclencheur en bas à gauche.
3. Dans le menu déroulant Sélectionner une source, sélectionnez Amazon MSK.
4. Ne configurez pas l'authentification.
5. Pour Cluster MSK, sélectionnez le nom de votre cluster.
6. Pour Taille de lot, saisissez 1. Cette étape facilite le test de cette fonctionnalité. Elle ne constitue pas une valeur idéale en production.
7. Pour Nom de la rubrique, indiquez le nom de votre rubrique Kafka.
8. Pour ID du groupe de consommateurs, indiquez l'ID de votre groupe de consommateurs Kafka.

Mettez à jour votre fonction d'événement Lambda pour lire vos données de streaming

Lambda fournit des informations sur les événements Kafka via le paramètre de méthode d'événement. Pour obtenir un exemple de structure d'un événement Amazon MSK, consultez the section called "Exemple d'évènement". Après avoir compris comment interpréter les événements Amazon MSK transférés par Lambda, vous pouvez modifier le code de votre fonction d'événement Lambda pour utiliser les informations qu'ils fournissent.

Fournissez le code suivant à votre fonction d'événement Lambda pour enregistrer le contenu d'un événement Lambda Amazon MSK à des fins de test :

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement Amazon MSK avec Lambda en utilisant .NET.

```
using System.Text;
using Amazon.Lambda.Core;
using Amazon.Lambda.KafkaEvents;


// Assembly attribute to enable the Lambda function's JSON input to be converted
 into a .NET class.
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSeri

namespace MSKLambda;

public class Function
{


    /// <param name="input">The event for the Lambda function handler to
 process.</param>
    /// <param name="context">The ILambdaContext that provides methods for
 logging and describing the Lambda environment.</param>
    /// <returns></returns>
    public void FunctionHandler(KafkaEvent evnt, ILambdaContext context)
    {

        foreach (var record in evnt.Records)
        {
            Console.WriteLine("Key:" + record.Key);
            foreach (var eventRecord in record.Value)
            {
                var valueBytes = eventRecord.Value.ToArray();
                var valueText = Encoding.UTF8.GetString(valueBytes);

                Console.WriteLine("Message:" + valueText);
            }
        }
    }


}
```

Go

Kit SDK pour Go V2

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement Amazon MSK avec Lambda en utilisant Go.

```
package main

import (
 "encoding/base64"
 "fmt"

 "github.com/aws/aws-lambda-go/events"
 "github.com/aws/aws-lambda-go/lambda"
)

func handler(event events.KafkaEvent) {
 for key, records := range event.Records {
  fmt.Println("Key:", key)

  for _, record := range records {
   fmt.Println("Record:", record)

   decodedValue, _ := base64.StdEncoding.DecodeString(record.Value)
   message := string(decodedValue)
   fmt.Println("Message:", message)
  }
 }
}

func main() {
 lambda.Start(handler)
}
```

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement Amazon MSK avec Lambda en utilisant Java.

```
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.KafkaEvent;
import com.amazonaws.services.lambda.runtime.events.KafkaEvent.KafkaEventRecord;

import java.util.Base64;
import java.util.Map;

public class Example implements RequestHandler<KafkaEvent, Void> {

    @Override
    public Void handleRequest(KafkaEvent event, Context context) {
        for (Map.Entry<String, java.util.List<KafkaEventRecord>> entry :
 event.getRecords().entrySet()) {
            String key = entry.getKey();
            System.out.println("Key: " + key);

            for (KafkaEventRecord record : entry.getValue()) {
                System.out.println("Record: " + record);

                byte[] value = Base64.getDecoder().decode(record.getValue());
                String message = new String(value);
                System.out.println("Message: " + message);
            }
        }

        return null;
    }
}
```

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Utilisation d'un événement Amazon MSK avec JavaScript Lambda à l'aide de.

```
exports.handler = async (event) => {
    // Iterate through keys
    for (let key in event.records) {
      console.log('Key: ', key)
      // Iterate through records
      event.records[key].map((record) => {
        console.log('Record: ', record)
        // Decode base64
        const msg = Buffer.from(record.value, 'base64').toString()
        console.log('Message:', msg)
      })
    }
}
```

Utilisation d'un événement Amazon MSK avec TypeScript Lambda à l'aide de.

```
import { MSKEvent, Context } from "aws-lambda";
import { Buffer } from "buffer";
import { Logger } from "@aws-lambda-powertools/logger";

const logger = new Logger({
  logLevel: "INFO",
  serviceName: "msk-handler-sample",
});

export const handler = async (
```

```
  event: MSKEvent,
  context: Context
): Promise<void> => {
  for (const [topic, topicRecords] of Object.entries(event.records)) {
    logger.info(`Processing key: ${topic}`);

    // Process each record in the partition
    for (const record of topicRecords) {
      try {
        // Decode the message value from base64
        const decodedMessage = Buffer.from(record.value, 'base64').toString();

        logger.info({
          message: decodedMessage
        });
      }
      catch (error) {
        logger.error('Error processing event', { error });
        throw error;
      }
    };
  }
}
```

PHP

Kit SDK pour PHP

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement Amazon MSK avec Lambda en utilisant PHP.

```
<?php
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0

// using bref/bref and bref/logger for simplicity
```

```
use Bref\Context\Context;
use Bref\Event\Kafka\KafkaEvent;
use Bref\Event\Handler as StdHandler;
use Bref\Logger\StderrLogger;

require __DIR__ . '/vendor/autoload.php';

class Handler implements StdHandler
{
    private StderrLogger $logger;
    public function __construct(StderrLogger $logger)
    {
        $this->logger = $logger;
    }

    /**
     * @throws JsonException
     * @throws \Bref\Event\InvalidLambdaEvent
     */
    public function handle(mixed $event, Context $context): void
    {
        $kafkaEvent = new KafkaEvent($event);
        $this->logger->info("Processing records");
        $records = $kafkaEvent->getRecords();

        foreach ($records as $record) {
            try {
                $key = $record->getKey();
                $this->logger->info("Key: $key");

                $values = $record->getValue();
                $this->logger->info(json_encode($values));

                foreach ($values as $value) {
                    $this->logger->info("Value: $value");
                }

            } catch (Exception $e) {
                $this->logger->error($e->getMessage());
            }
        }
        $totalRecords = count($records);
        $this->logger->info("Successfully processed $totalRecords records");
```

```
    }
}

$logger = new StderrLogger();
return new Handler($logger);
```

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement Amazon MSK avec Lambda en utilisant Python.

```
import base64

def lambda_handler(event, context):
    # Iterate through keys
    for key in event['records']:
        print('Key:', key)
        # Iterate through records
        for record in event['records'][key]:
            print('Record:', record)
            # Decode base64
            msg = base64.b64decode(record['value']).decode('utf-8')
            print('Message:', msg)
```

Ruby

Kit SDK pour Ruby

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement Amazon MSK avec Lambda en utilisant Ruby.

```
require 'base64'

def lambda_handler(event:, context:)
  # Iterate through keys
  event['records'].each do |key, records|
    puts "Key: #{key}"

    # Iterate through records
    records.each do |record|
      puts "Record: #{record}"

      # Decode base64
      msg = Base64.decode64(record['value'])
      puts "Message: #{msg}"
    end
  end
end
```

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement Amazon MSK avec Lambda en utilisant Rust.

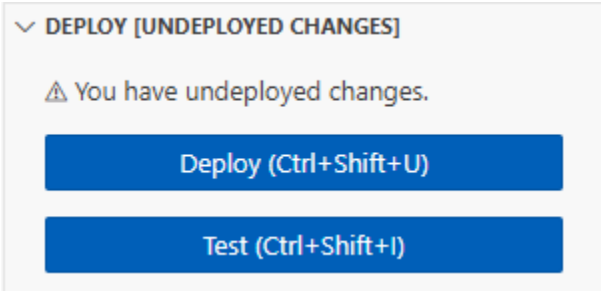
```
use aws_lambda_events::event::kafka::KafkaEvent;
use lambda_runtime::{run, service_fn, tracing, Error, LambdaEvent};
use base64::prelude::*;
use serde_json::{Value};
use tracing::{info};

/// Pre-Requisites:
/// 1. Install Cargo Lambda - see https://www.cargo-lambda.info/guide/getting-
started.html
/// 2. Add packages tracing, tracing-subscriber, serde_json, base64
///
/// This is the main body for the function.
/// Write your code inside it.
/// There are some code example in the following URLs:
/// - https://github.com/awslabs/aws-lambda-rust-runtime/tree/main/examples
/// - https://github.com/aws-samples/serverless-rust-demo/

async fn function_handler(event: LambdaEvent<KafkaEvent>) -> Result<Value, Error>
 {

    let payload = event.payload.records;

    for (_name, records) in payload.iter() {

        for record in records {

         let record_text = record.value.as_ref().ok_or("Value is None")?;
         info!("Record: {}", &record_text);

         // perform Base64 decoding
         let record_bytes = BASE64_STANDARD.decode(record_text)?;
         let message = std::str::from_utf8(&record_bytes)?;

         info!("Message: {}", message);
        }

    }

    Ok(().into())
}

#[tokio::main]
```

```
async fn main() -> Result<(), Error> {

    // required to enable CloudWatch error logging by the runtime
    tracing::init_default_subscriber();
    info!("Setup CW subscriber!");

    run(service_fn(function_handler)).await
}
```

Vous pouvez fournir le code de fonction à votre fonction Lambda à l'aide de la console.

Pour mettre à jour le code de fonction à l'aide de l'éditeur de code de la console

1. Ouvrez la page Event Functions de la console Lambda et sélectionnez votre fonction.
2. Sélectionnez l'onglet Code.
3. Dans le volet Source du code, sélectionnez votre fichier de code source et modifiez-le dans l'éditeur de code intégré.
4. Dans la section DÉPLOYER, choisissez Déployer pour mettre à jour le code de votre fonction :



Testez votre fonction d'événement Lambda pour vérifier qu'elle est connectée à votre rubrique Amazon MSK

Vous pouvez désormais vérifier si votre Lambda est invoqué par la source d'événements en consultant les journaux d'événements. CloudWatch

Pour vérifier si votre fonction d'événement Lambda est invoquée

1. Utilisez votre hôte administrateur Kafka pour générer des événements Kafka à l'aide de la CLI `kafka-console-producer`. Pour plus d'informations, consultez Write some events into the topic dans la documentation Kafka. Envoyez suffisamment d'événements pour remplir le lot

défini en fonction de la taille du lot pour le mappage de votre source d'événements défini à l'étape précédente, ou Lambda attend des informations supplémentaires avant d'être invoquée.

2. Si votre fonction s'exécute, Lambda écrit ce qui s'est passé à. CloudWatch Dans la console, accédez à la page détaillée de votre fonction d'événement Lambda.
3. Sélectionnez l'onglet Configuration.
4. Dans la barre latérale, sélectionnez Outils de surveillance et d'exploitation.
5. Identifiez le groupe de CloudWatch journaux sous Configuration de la journalisation. Le groupe de journaux doit commencer par `/aws/lambda`. Choisissez le lien vers le groupe de journaux.
6. Dans la CloudWatch console, examinez les événements du journal pour les événements du journal que Lambda a envoyés au flux de journal. Identifiez s'il existe des événements de journaux contenant le message de votre événement Kafka, comme dans l'image suivante. Si tel est le cas, vous avez connecté avec succès une fonction d'événement Lambda à Amazon MSK à l'aide d'un mappage de source d'événements Lambda.

Utilisation de Lambda avec Apache Kafka autogéré

Cette rubrique décrit comment utiliser Lambda avec un cluster Kafka autogéré. En AWS termes terminologiques, un cluster autogéré inclut les clusters Kafka non AWS hébergés. Par exemple, vous pouvez héberger votre cluster Kafka avec un fournisseur de cloud tel que Confluent Cloud ou Redpanda.

Ce chapitre explique comment utiliser un cluster Apache Kafka autogéré comme source d'événements pour votre fonction d'événement Lambda. Le processus général d'intégration d'Apache Kafka autogéré à Lambda comprend les étapes suivantes :

1. Configuration du cluster et du réseau : configurez d'abord votre cluster Apache Kafka autogéré avec la configuration réseau appropriée pour permettre à Lambda d'accéder à votre cluster.
2. Configuration du mappage des sources d'événements : créez ensuite la ressource de mappage des sources d'événements dont Lambda a besoin pour connecter de façon sécurisée votre cluster Apache Kafka à votre fonction.
3. Configuration de la fonction événementielle et des autorisations — Enfin, assurez-vous que votre fonction est correctement configurée et qu'elle dispose des autorisations nécessaires dans son rôle d'exécution.

Apache Kafka en tant que source d'événement fonctionne de la même manière qu'Amazon Simple Queue Service (Amazon SQS) ou Amazon Kinesis. Lambda interroge en interne les nouveaux messages provenant de la source de l'événement, puis invoque de manière synchrone la fonction d'événement Lambda cible. Lambda lit les messages par lot et les fournit à votre fonction en tant que charge utile d'événement. La taille maximale du lot est configurable (la valeur par défaut est de 100 messages). Pour plus d'informations, consultez the section called "Comportement de traitement par lots".

Pour optimiser le débit de votre mappage des sources d'événements Apache Kafka autogéré, configurez le mode alloué. En mode alloué, vous pouvez définir le nombre minimal et maximal de sondeurs d'événements alloués à votre mappage des sources d'événements. Cela peut améliorer la capacité de votre mappage des sources d'événements à gérer les pics de messages inattendus. Pour de plus amples informations, veuillez consulter Mode alloué.

> **Warning**
>
> Les mappages des sources d'événements Lambda traitent chaque événement au moins une fois, et le traitement des enregistrements peut être dupliqué. Pour éviter les problèmes

potentiels liés à des événements dupliqués, nous vous recommandons vivement de rendre votre code de fonction idempotent. Pour en savoir plus, consultez Comment rendre ma fonction Lambda idempotente dans le Knowledge Center. AWS

Pour les sources d' Kafka-based événements, Lambda prend en charge les paramètres de contrôle du traitement, tels que les fenêtres de traitement par lots et la taille des lots. Pour plus d'informations, consultez Comportement de traitement par lots.

Pour un exemple d'utilisation de Kafka autogéré comme source d'événements, consultez la section Utilisation d'Apache Kafka auto-hébergée comme source d'événements AWS Lambda sur le blog Compute. AWS

Rubriques

- Exemple d'évènement
- Configuration de votre cluster Apache Kafka autogéré et de votre réseau Lambda
- Configuration des autorisations de rôle d'exécution Lambda
- Configuration de sources d'événements Apache Kafka autogérées pour Lambda

Exemple d'évènement

Lambda envoie le lot de messages dans le paramètre d'événement lorsqu'il invoque votre fonction d'événement Lambda. La charge utile d'un événement contient un tableau de messages. Chaque élément de tableau contient des détails de la rubrique Kafka et l'identifiant de partition Kafka, ainsi qu'un horodatage et un message codé en base 64.

```
{
   "eventSource": "SelfManagedKafka",
   "bootstrapServers":"b-2.demo-cluster-1.a1bcde.c1.kafka.us-
east-1.amazonaws.com:9092,b-1.demo-cluster-1.a1bcde.c1.kafka.us-
east-1.amazonaws.com:9092",
   "records":{
      "mytopic-0":[
         {
            "topic":"mytopic",
            "partition":0,
            "offset":15,
            "timestamp":1545084650987,
```

```
            "timestampType":"CREATE_TIME",
            "key":"abcDEFghiJKLmnoPQRstuVWXyz1234==",
            "value":"SGVsbG8sIHRoaXMgaXMgYSB0ZXN0Lg==",
            "headers":[
               {
                  "headerKey":[
                     104,
                     101,
                     97,
                     100,
                     101,
                     114,
                     86,
                     97,
                     108,
                     117,
                     101
                  ]
               }
            ]
         }
      ]
   }
}
```

Configuration de votre cluster Apache Kafka autogéré et de votre réseau Lambda

Pour connecter votre fonction d'événement Lambda à votre cluster Apache Kafka autogéré, vous devez configurer correctement votre cluster et le réseau dans lequel il réside. Cette page décrit comment configurer votre cluster et votre réseau. Si votre cluster et votre réseau sont déjà correctement configurés, consultez the section called “Configurer une source d’événements” pour configurer le mappage des sources d’événements.

Rubriques

- Self-managed Configuration du cluster Apache Kafka
- Configurer la sécurité réseau

Self-managed Configuration du cluster Apache Kafka

Vous pouvez héberger votre cluster Apache Kafka autogéré auprès de fournisseurs de cloud comme Confluent Cloud ou Redpanda, ou l’exécuter sur votre propre infrastructure. Assurez-vous que votre

cluster est correctement configuré et accessible depuis le réseau auquel se connecte votre mappage de source d'événements Lambda.

Configurer la sécurité réseau

Pour donner à Lambda un accès complet à Apache Kafka autogéré via votre mappage des sources d'événements, soit votre cluster doit utiliser un point de terminaison public (adresse IP publique), soit vous devez fournir un accès au VPC Amazon dans lequel vous avez créé le cluster.

Lorsque vous utilisez Apache Kafka autogéré avec Lambda, créez des points de terminaison AWS PrivateLink VPC qui fournissent à votre fonction d'événement un accès aux ressources de votre Amazon VPC.

> **Note**
>
> AWS PrivateLink Les points de terminaison VPC sont requis pour les fonctions avec des mappages de sources d'événements qui utilisent le mode par défaut (à la demande) pour les sondeurs d'événements. Si le mappage de votre source d'événements utilise le mode provisionné, vous n'avez pas besoin de configurer les points de terminaison AWS PrivateLink VPC.

Créez un point de terminaison pour accéder aux ressources suivantes :

- Lambda — Créez un point de terminaison pour le principal de service Lambda.
- AWS STS — Créez un point de terminaison pour le AWS STS afin qu'un directeur de service assume un rôle en votre nom.
- Secrets Manager : si votre cluster utilise Secrets Manager pour stocker les informations d'identification, créez un point de terminaison pour Secrets Manager.

Vous pouvez également configurer une passerelle NAT sur chaque sous-réseau public d'Amazon VPC. Pour plus d'informations, consultez the section called “Accès Internet pour les fonctions VPC”.

Lorsque vous créez un mappage des sources d'événements pour Apache Kafka autogéré, Lambda vérifie si des interfaces réseau Elastic (ENI) sont déjà présentes pour les sous-réseaux et les groupes de sécurité configurés pour votre VPC Amazon. Si Lambda trouve des ENI existantes, il tente de les réutiliser. Sinon, Lambda crée de nouvelles ENI pour se connecter à la source d'événement et invoquer votre fonction.

> **Note**
>
> Les fonctions d'événement Lambda s'exécutent toujours dans des VPC appartenant au service Lambda. La configuration VPC de votre fonction n'affecte pas le mappage des sources d'événements. Seule la configuration réseau des sources d'événements détermine la manière dont Lambda se connecte à votre source d'événements.

Configurez les groupes de sécurité pour le VPC Amazon contenant votre cluster. Par défaut, Apache Kafka autogéré utilise les ports suivants : `9092`.

- Règles entrantes – Autorisent tout le trafic sur le port de l'agent par défaut pour le groupe de sécurité associé à votre source d'événement. Vous pouvez également utiliser une règle de groupe de sécurité avec référence circulaire pour autoriser l'accès à partir d'instances appartenant au même groupe de sécurité.
- Règles de sortie : autorisez tout le trafic sur le port `443` pour les destinations externes si votre fonction doit communiquer avec les AWS services. Vous pouvez également utiliser une règle de groupe de sécurité à référencement automatique pour limiter l'accès au courtier si vous n'avez pas besoin de communiquer avec d'autres AWS services.
- Règles entrantes relatives au point de terminaison Amazon VPC – Si vous utilisez un point de terminaison Amazon VPC, le groupe de sécurité associé à votre point de terminaison Amazon VPC doit autoriser le trafic entrant sur le port `443` en provenance du groupe de sécurité du cluster.

Si votre cluster utilise l'authentification, vous pouvez également restreindre la politique de point de terminaison pour le point de terminaison Secrets Manager. Pour appeler l'API Secrets Manager, Lambda utilise votre rôle de fonction, et non le principal de service Lambda.

Example Politique de point de terminaison de VPC — Point de terminaison Secrets Manager

```
{
      "Statement": [
          {
              "Action": "secretsmanager:GetSecretValue",
              "Effect": "Allow",
              "Principal": {
                  "AWS": [
                      "arn:aws::iam::123456789012:role/my-role"
                  ]
```

```
            },
            "Resource": "arn:aws::secretsmanager:us-west-2:123456789012:secret:my-
secret"
        }
    ]
}
```

Lorsque vous utilisez des points de terminaison Amazon VPC, AWS achemine vos appels d'API pour appeler votre fonction à l'aide de l'Elastic Network Interface (ENI) du point de terminaison. Le principal de service Lambda doit appeler `lambda:InvokeFunction` pour tous les rôles et fonctions utilisant ces ENI.

Par défaut, les points de terminaison Amazon VPC disposent de politiques IAM ouvertes qui permettent un accès étendu aux ressources. La meilleure pratique consiste à restreindre ces politiques pour effectuer les actions nécessaires à l'aide de ce point de terminaison. Pour garantir que le mappage de votre source d'événements est en mesure d'appeler votre fonction d'événement Lambda, la politique de point de terminaison VPC doit autoriser le principal du service Lambda à appeler et. `sts:AssumeRole` `lambda:InvokeFunction` Le fait de restreindre vos politiques de point de terminaison de VPC pour autoriser uniquement les appels d'API provenant de votre organisation empêche le mappage des sources d'événements de fonctionner correctement. C'est pourquoi `"Resource": "*"` est requis dans ces politiques.

Les exemples de politiques de point de terminaison de VPC suivants montrent comment accorder l'accès requis au principal de service Lambda pour les points de terminaison AWS STS et Lambda.

Example Politique relative aux points de terminaison VPC — AWS STS point de terminaison

```
{
    "Statement": [
        {
            "Action": "sts:AssumeRole",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "lambda.amazonaws.com"
                ]
            },
            "Resource": "*"
        }
    ]
}
```

Example Politique de point de terminaison de VPC — Point de terminaison Lambda

```
{
      "Statement": [
          {
              "Action": "lambda:InvokeFunction",
              "Effect": "Allow",
              "Principal": {
                  "Service": [
                      "lambda.amazonaws.com"
                  ]
              },
              "Resource": "*"
          }
      ]
  }
```

Configuration des autorisations de rôle d’exécution Lambda

Outre l'accès à votre cluster Kafka autogéré, votre fonction d'événement Lambda a besoin d'autorisations pour effectuer diverses actions d'API. Ajoutez ces autorisations au rôle d’exécution de votre fonction. Si vos utilisateurs ont besoin d'accéder à des actions d'API, ajoutez les autorisations requises à la politique d'identité de l'utilisateur ou du rôle Gestion des identités et des accès AWS (IAM).

Rubriques

- Autorisations requises pour la fonction d'événement Lambda
- Autorisations facultatives relatives à la fonction d'événement Lambda
- Ajout d’autorisations à votre rôle d’exécution
- Octroi d’accès à des utilisateurs avec une politique IAM

Autorisations requises pour la fonction d'événement Lambda

Pour créer et stocker des journaux dans un groupe de CloudWatch journaux dans Amazon Logs, votre fonction d'événement Lambda doit disposer des autorisations suivantes dans son rôle d'exécution :

- journaux : CreateLogGroup
- journaux : CreateLogStream

- journaux : PutLogEvents

Autorisations facultatives relatives à la fonction d'événement Lambda

Votre fonction d'événement Lambda peut également avoir besoin d'autorisations pour :

- Décrivez votre secret Secrets Manager.
- Accédez à votre AWS Key Management Service (AWS KMS) clé gérée par le client.
- Accédez à votre Amazon VPC.
- Envoyez les enregistrements des invocations ayant échoué vers une destination.

Secrets Manager et AWS KMS des autorisations

Selon le type de contrôle d'accès que vous configurez pour vos courtiers Kafka, votre fonction Lambda Event peut avoir besoin d'une autorisation pour accéder à votre secret Secrets Manager ou pour déchiffrer AWS KMS votre clé gérée par le client. Afin d’accéder à ces ressources, le rôle d’exécution de votre fonction doit disposer des autorisations suivantes :

- responsable des secrets : GetSecretValue
- kms:Decrypt

Autorisations VPC

Si seuls les utilisateurs d'un VPC peuvent accéder à votre cluster Apache Kafka autogéré, votre fonction d'événement Lambda doit être autorisée à accéder à vos ressources Amazon VPC. Ces ressources incluent les sous-réseaux, groupes de sécurité et interfaces réseau de votre VPC. Afin d’accéder à ces ressources, le rôle d’exécution de votre fonction doit disposer des autorisations suivantes :

- EC2 : CreateNetworkInterface
- EC2 : DescribeNetworkInterfaces
- EC2 : DescribeVpcs
- EC2 : DeleteNetworkInterface
- EC2 : DescribeSubnets
- EC2 : DescribeSecurityGroups

Ajout d’autorisations à votre rôle d’exécution

Pour accéder aux autres AWS services utilisés par votre cluster Apache Kafka autogéré, Lambda utilise les politiques d'autorisation que vous définissez dans le rôle d'exécution de votre fonction d'événement Lambda.

Par défaut, Lambda n’est pas autorisé à exécuter les actions obligatoires ou facultatives pour un cluster Apache Kafka autogéré. Vous devez créer et définir ces actions dans une stratégie d’approbation IAM pour votre rôle d’exécution. Cet exemple montre comment créer une stratégie autorisant Lambda à accéder à vos ressources Amazon VPC.

JSON

```
{
        "Version":"2012-10-17",
        "Statement":[
           {
              "Effect":"Allow",
              "Action":[
                 "ec2:CreateNetworkInterface",
                 "ec2:DescribeNetworkInterfaces",
                 "ec2:DescribeVpcs",
                 "ec2:DeleteNetworkInterface",
                 "ec2:DescribeSubnets",
                 "ec2:DescribeSecurityGroups"
              ],
              "Resource":"*"
           }
        ]
    }
```

Octroi d’accès à des utilisateurs avec une politique IAM

Par défaut, les utilisateurs et les rôles n’ont pas l’autorisation d’effectuer des opérations d’API de source d’événement. Pour accorder l’accès aux utilisateurs de votre organisation ou de votre compte, vous pouvez ajouter ou mettre à jour une stratégie basée sur l’identité. Pour plus d'informations, consultez la section Contrôle de l'accès aux AWS ressources à l'aide de politiques dans le Guide de l'utilisateur IAM.

Pour résoudre les erreurs d'authentification et d'autorisation, consultez the section called "Résolution des problèmes".

Configuration de sources d'événements Apache Kafka autogérées pour Lambda

Pour utiliser un cluster Apache Kafka autogéré comme source d'événements pour votre fonction événementielle Lambda, vous devez créer un mappage des sources d'événements qui relie les deux ressources. Cette page explique comment créer un mappage des sources d'événements pour Apache Kafka autogéré.

Cette page suppose que vous avez déjà correctement configuré votre cluster Kafka et le réseau dans lequel il réside. Si vous devez configurer votre cluster ou votre réseau, consultez the section called "Configuration du cluster et du réseau".

Rubriques

- Utilisation d'un cluster Apache Kafka autogéré comme source d'événement
- Configuration des méthodes d'authentification de cluster dans Lambda
- Création d'un mappage des sources d'événements Lambda pour une source d'événements Apache Kafka autogéré
- Tous les paramètres de configuration des sources d'événements Apache Kafka autogéré dans Lambda

Utilisation d'un cluster Apache Kafka autogéré comme source d'événement

Lorsque vous ajoutez votre cluster Apache Kafka ou Amazon MSK comme déclencheur pour votre fonction événementielle Lambda, le cluster est utilisé comme source de l'événement.

Lambda lit les données d'événements des rubriques Kafka que vous spécifiez comme `Topics` dans un CreateEventSourceMapping demande, sur la base de position de départ que vous spécifiez. Lorsque le traitement a réussi, votre rubrique Kafka est validée dans votre cluster Kafka.

Lambda lit les messages séquentiellement pour chaque partition de rubrique Kafka. Une seule charge utile Lambda peut contenir des messages provenant de plusieurs partitions. Lorsque davantage d'enregistrements sont disponibles, Lambda continue à traiter les enregistrements par lots, en fonction de BatchSize valeur que vous spécifiez dans CreateEventSourceMapping demande, jusqu'à ce que votre fonction aborde le sujet.

Après avoir traité chaque lot, Lambda valide les décalages des messages dans celui-ci. Si votre fonction renvoie une erreur pour l'un des messages d'un lot, Lambda réessaie le lot de messages

complet jusqu'à ce que le traitement réussisse ou que les messages expirent. Vous pouvez envoyer les enregistrements qui échouent à toutes les tentatives vers une destination en cas de panne pour un traitement ultérieur.

> **Note**
>
> Alors que les fonctions événementielles Lambda ont généralement un délai d'expiration maximal de 15 minutes, les mappages de sources d'événements pour Amazon MSK, Apache Kafka autogéré, Amazon DocumentDB et Amazon MQ pour ActiveMQ et RabbitMQ ne prennent en charge que les fonctions dont le délai d'expiration maximal est de 14 minutes.

Configuration des méthodes d'authentification de cluster dans Lambda

Lambda prend en charge plusieurs méthodes d'authentification auprès de votre cluster Apache Kafka autogéré. Veillez à configurer le cluster Kafka pour utiliser l'une des méthodes d'authentification prises en charge suivantes : Pour de plus amples informations sur la sécurité, veuillez consulter la section Sécurité de la documentation Kafka.

SASL/SCRAM authentication

Lambda prend en charge l'authentification et la sécurité simples Layer/Salted Mécanisme d'authentification des réponses aux défis (SASL/SCRAM) authentification avec chiffrement TLS (Transport Layer Security) (`SASL_SSL`). Lambda envoie les informations d'identification chiffrées pour s'authentifier auprès du cluster. Lambda ne prend pas en charge SASL/SCRAM avec du texte en clair (`SASL_PLAINTEXT`). Pour plus d'informations sur SASL/SCRAM authentification, voir RÉFÉRENCE 5802.

Lambda prend également en charge SASL/PLAIN authentification. Comme ce mécanisme utilise des informations d'identification en texte clair, la connexion au serveur doit utiliser le chiffrement TLS pour garantir la protection des informations d'identification.

Pour l'authentification SASL, vous devez stocker les informations d'identification en tant que secret dans AWS Secrets Manager. Pour plus d'informations sur l'utilisation de Secrets Manager, voir Créez un AWS Secrets Manager secret dans le AWS Secrets Manager Guide de l'utilisateur.

> **Important**
>
> Pour utiliser Secrets Manager à des fins d'authentification, les secrets doivent être stockés dans le même AWS région comme fonction événementielle Lambda.

Authentification TLS mutuelle

Mutual TLS (mTLS) fournit une authentification bidirectionnelle entre le client et le serveur. Le client envoie un certificat au serveur pour que le serveur vérifie le client, et le serveur envoie un certificat au client pour que le client vérifie le serveur.

Dans Apache Kafka autogéré, Lambda agit en tant que client. Vous configurez un certificat client (en tant que secret dans Secrets Manager) pour authentifier Lambda auprès des courtiers Kafka. Le certificat client doit être signé par une autorité de certification dans le magasin d'approbations du serveur.

Le cluster Kafka envoie un certificat de serveur à Lambda pour authentifier les courtiers auprès de Lambda. Le certificat de serveur peut être un certificat CA public ou privé CA/self-signed certificat. Le certificat d'autorité de certification publique doit être signé par une autorité de certification située du magasin d'approbations Lambda. Pour un privé CA/self-signed certificat, vous configurez le certificat CA racine du serveur (en tant que secret dans Secrets Manager). Lambda utilise le certificat racine pour vérifier les courtiers Kafka.

Pour de plus amples informations sur mTLS, veuillez consulter Introduction d'une authentification TLS mutuelle pour Amazon MSK en tant que source d'événement.

Authentification OAuth 2.0

Supports Lambda SASL/OAUTHBEARER authentification avec chiffrement TLS (`SASL_SSL`). Lambda demande un jeton d'accès à votre fournisseur d'identité OAuth 2.0 et présente ce jeton à vos courtiers Kafka. Lambda actualise le jeton avant son expiration. Configurez vos courtiers pour qu'ils valident les jetons provenant du même fournisseur d'identité.

Pour utiliser cette méthode, choisissez `OAUTHBEARER_AUTH` en tant que `Type` d'un SourceAccessConfiguration et indiquez l'ARN du gestionnaire de secrets de votre secret OAuth dans le `URI` champ. Pour le contenu du secret, voir the section called "Configuration du secret OAuth".

Lambda prend en charge deux types de subventions. Les champs que vous stockez dans le secret déterminent celui que Lambda utilise.

- Informations d'identification du client — Lambda envoie un ID client et un code secret client au point de terminaison du jeton. Utilisez ce type d'autorisation lorsque votre fournisseur d'identité émet un secret client.
- porteur JWT — Lambda signe une assertion JSON Web Token (JWT) avec une clé privée et envoie l'assertion au point de terminaison du jeton. Utilisez ce type d'autorisation lorsque votre fournisseur d'identité attend une assertion signée au lieu d'un secret client.

Si votre fournisseur d'identité ou vos courtiers ont besoin de valeurs supplémentaires, indiquez chacune d'elles comme entrée de configuration d'accès à la source. Entrez la valeur littérale dans `URI` champ plutôt qu'un ARN secret.

- `OAUTHBEARER_SCOPE` — L'étendue demandée par Lambda lorsqu'il demande un jeton.
- `OAUTHBEARER_AUDIENCE` — L'audience que Lambda demande lorsqu'il demande un jeton.
- `OAUTHBEARER_LOGICAL_CLUSTER` — L'ID de cluster logique que Lambda envoie à vos courtiers en tant qu'extension SASL.
- `OAUTHBEARER_IDENTITY_POOL` — L'identifiant du pool d'identités que Lambda envoie à vos courtiers en tant qu'extension SASL.

> **Note**
>
> Ces quatre types nécessitent un type d'authentification OAuth 2.0. Fournissez-leur `OAUTHBEARER_AUTH`, ou fournissez uniquement `OAUTHBEARER_AUDIENCE` avec `IAM_OAUTHBEARER_AUTH`. Si vous fournissez l'un d'entre eux sans l'un de ces types d'authentification, Lambda renvoie une erreur de validation.

Si vos courtiers présentent un certificat signé par une autorité de certification privée, fournissez également `SERVER_ROOT_CA_CERTIFICATE` afin que Lambda puisse les vérifier. Pour plus d'informations, consultez the section called “Configuration du secret du certificat d'autorité de certification racine du serveur”.

Authentification IAM

Si votre cluster est un cluster Amazon MSK auquel vous accédez via votre propre configuration réseau, vous pouvez l'enregistrer en tant que source d'événements Kafka autogérée et vous authentifier auprès d'IAM. Les configurations réseau personnalisées incluent un nom de domaine

personnalisé devant vos courtiers ou une connexion depuis un autre compte. Lambda signe chaque connexion avec les informations d'identification du rôle d'exécution de votre fonction, de sorte que vous ne stockez aucune information d'identification dans Secrets Manager.

Pour utiliser cette méthode, activez le contrôle d'accès IAM sur votre cluster. Ensuite, choisissez `IAM_AUTH` en tant que `Type` d'une configuration d'accès à la source et omettez le `URI` champ. Le rôle d'exécution de votre fonction nécessite les autorisations de cluster décrites dans the section called “Configurer les autorisations ”.

Si vos courtiers présentent un certificat signé par une autorité de certification privée, fournissez également `SERVER_ROOT_CA_CERTIFICATE` afin que Lambda puisse les vérifier. Un nom de domaine personnalisé devant vos courtiers en a généralement besoin.

Authentification IAM avec SASL/OAUTHBEARER

Si vos courtiers acceptent les jetons OAuth 2.0, vous pouvez utiliser AWS en tant que fournisseur d'identité. Lambda présente un AWS jeton d'identité Web envoyé à vos courtiers SASL/OAUTHBEARER. Lambda demande un jeton de courte durée pour le rôle d'exécution de votre fonction avec `sts:GetWebIdentityToken` action, de sorte que vous ne stockez aucune information d'identification dans Secrets Manager. Lambda demande un nouveau jeton avant que le jeton actuel n'expire.

Pour utiliser cette méthode, choisissez `IAM_OAUTHBEARER_AUTH` en tant que `Type` d'une configuration d'accès à la source et omettez le `URI` champ. Vous devez également fournir `OAUTHBEARER_AUDIENCE` auprès du public attendu par vos courtiers. Le rôle d'exécution de votre fonction nécessite une autorisation pour appeler `sts:GetWebIdentityToken`.

Configurez vos courtiers pour qu'ils aient confiance AWS en tant que fournisseur d'identité OpenID Connect (OIDC) avant de créer le mappage des sources d'événements. Si vos courtiers ne font pas confiance à AWS émetteur, ils rejettent le jeton et Lambda ne peut pas lire les articles de vos sujets.

> **Note**
>
> `IAM_OAUTHBEARER_AUTH` supports uniquement `OAUTHBEARER_AUDIENCE`. Si vous fournissez également `OAUTHBEARER_SCOPE`, `OAUTHBEARER_LOGICAL_CLUSTER`, ou `OAUTHBEARER_IDENTITY_POOL`, Lambda renvoie une erreur de validation.

Configuration du secret du certificat client

Le secret CLIENT_CERTIFICATE_TLS_AUTH nécessite un champ de certificat et un champ de clé privée. Pour une clé privée chiffrée, le secret nécessite un mot de passe de clé privée. Le certificat et la clé privée doivent être au format PEM.

> **Note**
>
> Lambda prend en charge les algorithmes de chiffrement de clés privées PBES1 (mais pas PBES2).

Le champ de certificat doit contenir une liste de certificats, commençant par le certificat client, suivi de tous les certificats intermédiaires et se terminant par le certificat racine. Chaque certificat doit commencer sur une nouvelle ligne avec la structure suivante :

```
-----BEGIN CERTIFICATE-----
            <certificate contents>
-----END CERTIFICATE-----
```

Secrets Manager prend en charge les secrets jusqu'à 65 536 octets, ce qui offre suffisamment d'espace pour de longues chaînes de certificats.

La clé privée doit être au format PKCS #8, avec la structure suivante :

```
-----BEGIN PRIVATE KEY-----
             <private key contents>
-----END PRIVATE KEY-----
```

Pour une clé privée chiffrée, utilisez la structure suivante :

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
              <private key contents>
-----END ENCRYPTED PRIVATE KEY-----
```

L'exemple suivant affiche le contenu d'un secret pour l'authentification mTLS à l'aide d'une clé privée chiffrée. Pour une clé privée chiffrée, incluez le mot de passe de clé privée dans le secret.

```
{"privateKeyPassword":"testpassword",
```

```
"certificate":"-----BEGIN CERTIFICATE-----
MIIE5DCCAsygAwIBAgIRAPJdwaFaNRrytHBto0j5BA0wDQYJKoZIhvcNAQELBQAw
...
j0Lh4/+1HfgyE2KlmII36dg4IMzNjAFEBZiCRoPimO40s1cRqtFHXoal0QQbIlxk
cmUuiAii9R0=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIFgjCCA2qgAwIBAgIQdjNZd6uFf9hbNC5RdfmHrzANBgkqhkiG9w0BAQsFADBb
...
rQoiowbbk5wXCheYSANQIfTZ6weQTgiCHCCbuuMKNVS95FkXm0vqVD/YpXKwA/no
c8PH3PSoAaRwMMgOSA2ALJvbRz8mpg==
-----END CERTIFICATE-----",
"privateKey":"-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFKzBVBgkqhkiG9w0BBQ0wSDAnBgkqhkiG9w0BBQwwGgQUiAFcK5hT/X7Kjmgp
...
QrSekqF+kWzmB6nAfSzgO9IaoAaytLvNgGTckWeUkWn/V0Ck+LdGUXzAC4RxZnoQ
zp2mwJn2NYB7AZ7+imp0azDZb+8YG2aUCiyqb6PnnA==
-----END ENCRYPTED PRIVATE KEY-----"
}
```

Configuration du secret du certificat d'autorité de certification racine du serveur

Vous créez ce secret si vos courtiers Kafka utilisent le chiffrement TLS avec des certificats signés par une autorité de certification privée. Vous pouvez utiliser le cryptage TLS pour VPC, SASL/SCRAM, SASL/PLAIN, ou authentification mTLS.

Le secret du certificat d'autorité de certification racine du serveur nécessite un champ contenant le certificat d'autorité de certification racine du courtier Kafka au format PEM. La structure du secret est présentée dans l'exemple suivant.

```
{"certificate":"-----BEGIN CERTIFICATE-----
MIID7zCCAtegAwIBAgIBADANBgkqhkiG9w0BAQsFADCBmDELMAkGA1UEBhMCVVMx
EDAOBgNVBAgTB0FyaXpvbmExEzARBgNVBAcTClNjb3R0c2RhbGUxJTAjBgNVBAoT
HFN0YXJmaWVsZCBUZWNobm9sb2dpZXMsIEluYy4xOzA5BgNVBAMTMlN0YXJmaWVs
ZCBTZXJ2aWNlcyBSb290IENlcnRpZmljYXRlIEF1dG...
-----END CERTIFICATE-----"
}
```

Configuration du secret OAuth

Vous créez ce secret lorsque vous utilisez `OAUTHBEARER_AUTH`. Le secret est un document JSON. Chaque secret OAuth a besoin `oauthTokenEndpointUrl` et `oauthClientId`. Ajoutez les

champs pour un seul type de subvention. Si vous fournissez des champs provenant des deux types d'autorisation, Lambda renvoie une erreur de validation.

Champ	Obligatoire	Description
`oauthTokenEndpointUrl`	O	Le point de terminaison du jeton de votre fournisseur d'identité. Il doit s'agir d'une URL HTTPS.
`oauthClientId`	O	L'identifiant client que votre fournisseur d'identité a émis.
`oauthClientSecret`	Informations d'identification du client uniquement	Le secret client émis par votre fournisseur d'identité.
`oauthClientEmail`	Support JWT uniquement	L'identité du compte de service que Lambda met dans l'assertion JWT.
`oauthPrivateKey`	Support JWT uniquement	La clé privée que Lambda utilise pour signer l'assertion JWT, au format PEM.
`oauthTokenExpirationSeconds`	N	Durée de vie de l'assertion JWT signée par Lambda. S'applique uniquement au type de subvention JWT bearer.
`oauthIdpCaCertificate`	N	Le certificat CA racine de votre fournisseur d'identité, au format PEM. Fournissez-le si votre fournisseur d'identité présente un certificat signé par une autorité de certification privée.

L'exemple suivant montre un secret pour le type d'autorisation des informations d'identification du client.

```
{"oauthTokenEndpointUrl":"https://idp.example.com/oauth2/token",
"oauthClientId":"my-client-id",
"oauthClientSecret":"my-client-secret"}
```

L'exemple suivant montre un secret pour le type de subvention JWT bearer.

```
{"oauthTokenEndpointUrl":"https://idp.example.com/oauth2/token",
"oauthClientId":"my-client-id",
"oauthClientEmail":"my-service-account@example.com",
"oauthPrivateKey":"-----BEGIN PRIVATE KEY-----
<private key contents>
-----END PRIVATE KEY-----"}
```

> **Important**
>
> Stockez le secret dans le même AWS Région comme fonction Lambda. Lambda lit le secret avec le rôle d'exécution de votre fonction, de sorte que ce rôle a besoin `secretsmanager:GetSecretValue` autorisation sur le secret.

Vous pouvez alterner les informations d'identification dans le secret sans recréer le mappage des sources d'événements. Lambda récupère les nouvelles valeurs et demande un nouveau jeton.

Création d'un mappage des sources d'événements Lambda pour une source d'événements Apache Kafka autogéré

Pour créer un mappage des sources d'événements, vous pouvez utiliser la console Lambda, AWS Command Line Interface (CLI) ou un SDK AWS.

Les étapes de console suivantes permettent d'ajouter un cluster Apache Kafka autogéré comme déclencheur pour votre fonction d'événement Lambda. En arrière-plan, cela crée une ressource de mappage des sources d'événements.

Conditions préalables

- Cluster Apache Kafka autogéré. Lambda prend en charge Apache Kafka versions 0.10.1.0 et ultérieures.

- Un rôle d'exécution avec l'autorisation d'accéder au AWS ressources utilisées par votre cluster Kafka autogéré.

Ajout d'un cluster Kafka autogéré (console)

Suivez ces étapes pour ajouter votre cluster Apache Kafka autogéré et une rubrique Kafka comme déclencheur pour votre fonction d'événement Lambda.

Pour ajouter un déclencheur Apache Kafka à votre fonction événementielle Lambda (console)

1. Ouvrez le Page des fonctions de l'événement de la console Lambda.
2. Choisissez le nom de votre fonction d'événement Lambda.
3. Sous Function overview (Vue d'ensemble de la fonction), choisissez Add trigger (Ajouter un déclencheur).
4. Sous Trigger configuration (Configuration du déclencheur), procédez comme suit :

    a. Choisissez le type de déclencheur Apache Kafka.

    b. Pour Bootstrap servers (Serveurs d'amorçage), entrez l'adresse de paire hôte et port d'un agent Kafka dans votre cluster, puis choisissez Add (Ajouter). Répétez l'opération pour chaque agent Kafka dans le cluster.

    c. Pour Topic name (Nom de rubrique), entrez le nom de la rubrique Kafka utilisée pour stocker les registres dans le cluster.

    d. Si vous configurez le mode provisionné, entrez une valeur pour Nombre minimum de participants à l'événement, une valeur pour Nombre maximum de participants à l'événement, et une valeur facultative pour PollerGroupName pour spécifier le regroupement de plusieurs ESM au sein d'un même VPC source d'événements.

    e. (Facultatif) Pour Batch size (Taille de lot), entrez le nombre maximal de registres à recevoir dans un même lot.

    f. Pour Batch window, veuillez saisir l'intervalle de temps maximal en secondes nécessaire à Lambda pour collecter des enregistrements avant d'invoquer la fonction.

    g. (Facultatif) Pour l'identifiant de groupe de consommateurs, entrez l'identifiant d'un groupe de consommateurs Kafka à rejoindre.

    h. (Facultatif) Pour Position de départ, choisissez Dernier pour commencer à lire le flux à partir du dernier enregistrement, Supprimer l'horizon pour commencer au premier enregistrement disponible ou À l'horodatage pour spécifier un horodatage à partir duquel commencer la lecture.

i. (Facultatif) Pour VPC, choisissez l’Amazon VPC pour votre cluster Kafka. Ensuite, choisissez le VPC subnets (Sous-réseaux VPC) et les VPC security groups (Groupes de sécurité VPC).

   Ce paramètre est requis si seuls des utilisateurs au sein de votre VPC accèdent à vos courtiers.

j. (Facultatif) Pour Authentication (Authentification), choisissez Add (Ajouter), puis procédez comme suit :

   i. Choisissez le protocole d’accès ou d’authentification des courtiers Kafka dans votre cluster.

      - Si votre courtier Kafka utilise SASL/PLAIN authentification, choisissez AUTHENTIFICATION_DE BASE.
      - Si votre courtier utilise SASL/SCRAM authentification, choisissez l'une des SASL_SCRAM protocoles.
      - Si vous configurez l’authentification mTLS, choisissez le protocole CLIENT_CERTIFICATE_TLS_AUTH.
      - Si votre courtier utilise OAuth 2.0, choisissez OAUTHBEARER_AUTH.
      - Si votre courtier utilise le contrôle d'accès IAM, choisissez IAM_AUTH.
      - Si votre courtier accepte AWS jetons d'identité Web sur OAuth 2.0, choisissez IAM_OAUTHBEARER_AUTH.

   ii. Pour SASL/SCRAM, mTLS ou OAuth 2.0, choisissez la clé secrète Secrets Manager qui contient les informations d'identification de votre cluster Kafka. IAM et IAM avec SASL/OAUTHBEARER l'authentification n'utilise pas de secret.

k. (Facultatif) Pour Encryption (Chiffrement), choisissez le secret Secrets Manager contenant le certificat d’autorité de certification racine que vos courtiers Kafka utilisent pour le chiffrement TLS, si vos courtiers Kafka utilisent des certificats signés par une autorité de certification privée.

   Ce paramètre s'applique au chiffrement TLS pour SASL/SCRAM ou SASL/PLAIN, et à l'authentification mTLS.

l. Pour créer le déclencheur dans un état désactivé pour le test (recommandé), désactivez Enable trigger (Activer le déclencheur). Ou, pour activer le déclencheur immédiatement, sélectionnezActiver un déclencheur.

5. Pour créer le déclencheur, choisissez Add (Ajouter).

Ajout d'un cluster Kafka autogéré (AWS CLI)

Utilisez l'exemple suivant AWS CLI commandes pour créer et afficher un déclencheur Apache Kafka autogéré pour votre fonction événementielle Lambda.

En utilisant SASL/SCRAM

Si les utilisateurs de Kafka accèdent à vos courtiers Kafka via Internet, spécifiez le secret Secrets Manager que vous avez créé pour SASL/SCRAM authentification. L'exemple suivant utilise créer un mappage des sources d'événements AWS CLI commande pour mapper une fonction événementielle Lambda nommée `my-kafka-function` à un sujet de Kafka nommé `AWSKafkaTopic`.

```
aws lambda create-event-source-mapping \
  --topics AWSKafkaTopic \
  --source-access-configuration Type=SASL_SCRAM_512_AUTH,URI=arn:aws:secretsmanager:us-
east-1:111122223333:secret:MyBrokerSecretName \
  --function-name arn:aws:lambda:us-east-1:111122223333:function:my-kafka-function \
  --self-managed-event-source '{"Endpoints":{"KAFKA_BOOTSTRAP_SERVERS":
["abc3.xyz.com:9092", "abc2.xyz.com:9092"]}}'
```

Utilisation d’un VPC

Si seuls des utilisateurs de Kafka au sein de votre VPC accèdent à vos agents Kafka, vous devez spécifier votre VPC, vos sous-réseaux et votre groupe de sécurité de VPC. L'exemple suivant utilise le créer un mappage des sources d'événements AWS CLI commande pour mapper une fonction événementielle Lambda nommée `my-kafka-function` à un sujet de Kafka nommé `AWSKafkaTopic`.

```
aws lambda create-event-source-mapping \
  --topics AWSKafkaTopic \
  --source-access-configuration '[{"Type": "VPC_SUBNET", "URI":
 "subnet:subnet-0011001100"}, {"Type": "VPC_SUBNET", "URI":
 "subnet:subnet-0022002200"}, {"Type": "VPC_SECURITY_GROUP", "URI":
 "security_group:sg-0123456789"}]' \
  --function-name arn:aws:lambda:us-east-1:111122223333:function:my-kafka-function \
  --self-managed-event-source '{"Endpoints":{"KAFKA_BOOTSTRAP_SERVERS":
["abc3.xyz.com:9092", "abc2.xyz.com:9092"]}}'
```

Affichage de l'état à l'aide du AWS CLI

L'exemple suivant utilise obtenir le mappage de la source de l'événement AWS CLI commande pour décrire l'état du mappage des sources d'événements que vous avez créé.

```
aws lambda get-event-source-mapping
              --uuid dh38738e-992b-343a-1077-3478934hjkfd7
```

Tous les paramètres de configuration des sources d’événements Apache Kafka autogéré dans Lambda

Tous les types de sources d'événements Lambda partagent les mêmes valeurs CreateEventSourceMapping et UpdateEventSourceMapping Opérations d'API. Cependant, seuls certains paramètres s’appliquent à Apache Kafka autogéré, comme indiqué dans le tableau suivant.

Paramètre	Obligatoire	Par défaut	Remarques
BatchSize	N	100	Maximum : 10 000.
SelfManagedKafkaEventSourceConfig.ConsumptionMode	N	Flux	`Stream` ou `Queue`. Détermine la façon dont Lambda utilise les enregistrements de la rubrique. Ne peut être défini que sur Créer. Quand `Queue`, `StartingPosition` , `StartingPositionTimestamp` , et `MaximumBatchingWindowInSeconds` ne pas appliquer. Pour plus de détails, consultez Interroger

Paramètre	Obligatoire	Par défaut	Remarques
			les sujets de Kafka en mode file d'attente.
DestinationConfig	N	N/A	the section called “Conserver les appels ayant échoué”
Activé	N	True	
FilterCriteria	N	N/A	Contrôlez les événements que Lambda envoie à votre fonction d'événement
FunctionName	O	N/A	
KMSKeyArn	N	N/A	the section called “Chiffrement des critères de filtre”
MaximumBatchingWindowInSeconds	N	500 ms	Comportement de traitement par lots Ne s'applique pas lorsque `ConsumptionMode` est `Queue`.

Paramètre	Obligatoire	Par défaut	Remarques
ProvisionedPollers Config	N	`MinimumPollers` : la valeur par défaut, si elle n'est pas spécifiée, est de 1 `MaximumPollers` : la valeur par défaut, si elle n'est pas spécifiée, est de 200 `PollerGroupName` : N/A	the section called "Mode alloué"
SelfManagedEventSource	O	N/A	Liste des agents Kafka. Peut définir uniquement sur Create (Créer)
SelfManagedKafkaEventSourceConfig	N	Contient le ConsumerGroupId champ dont la valeur par défaut est unique.	Peut définir uniquement sur Create (Créer)
SourceAccessConfigurations	N	Pas d'informations d'identification	Informations sur le VPC ou informations d'authentification pour le cluster Pour SASL_PLAIN, définissez la valeur BASIC_AUTH

Paramètre	Obligatoire	Par défaut	Remarques
StartingPosition	Y (mode Stream uniquement)	N/A	AT_TIMESTAMP, TRIM_HORIZON ou DERNIER Peut définir uniquement sur Create (Créer) Ne s'applique pas lorsque `ConsumptionMode` est `Queue`.
StartingPositionTimestamp	N	N/A	Obligatoire si StartingPosition est défini sur AT_TIMESTAMP Ne s'applique pas lorsque `ConsumptionMode` est `Queue`.
Étiquettes	N	N/A	the section called “Balises de mappage des sources d’événements”
Rubriques	O	N/A	Nom de la rubrique Peut définir uniquement sur Create (Créer)

> **Note**
>
> Lorsque vous spécifiez un `PollerGroupName`, plusieurs ESM au sein d'un même Amazon VPC peuvent partager la capacité de l'Event Poller Unit (EPU). Vous pouvez utiliser cette

option pour optimiser les coûts du mode provisionné pour vos ESM. Exigences relatives au regroupement ESM :

- Les ESM doivent se trouver dans le même Amazon VPC
- Maximum de 100 ESM par groupe de sondeurs
- Le nombre maximum total de personnes interrogées dans tous les ESM d'un groupe ne peut pas dépasser 2 000

Vous pouvez mettre à jour le `PollerGroupName` pour déplacer un ESM vers un autre groupe, ou supprimer un ESM d'un groupe en définissant `PollerGroupName` vers une chaîne vide (« »).

Modes de mise à l'échelle des sondeurs d'événements Apache Kafka dans Lambda

Vous pouvez choisir entre deux modes de mise à l'échelle des sondeurs d'événements pour Amazon MSK et les mappages des sources d'événements Apache Kafka autogéré :

- On-demand mode (par défaut)
- Mode alloué

On-demand mode (par défaut)

Lorsque vous créez initialement une source d'événement Kafka, Lambda alloue un nombre de sondeurs d'événements par défaut pour traiter toutes les partitions de la rubrique Kafka. Lambda augmente ou diminue automatiquement le nombre de sondeurs d'événements, en fonction de la charge de messages.

Toutes les minutes, Lambda évalue le décalage entre toutes les partitions dans la rubrique. Si le décalage est trop élevé, la partition reçoit des messages plus rapidement que Lambda ne peut les traiter. Si nécessaire, Lambda ajoute ou supprime des sondeurs d'événements dans la rubrique. Cette mise à l'échelle automatique consistant à ajouter ou à supprimer des sondeurs d'événements a lieu dans les trois minutes suivant l'évaluation.

Si votre fonction d'événement Lambda cible est limitée, Lambda réduit le nombre de sondeurs d'événements. Cette action réduit la charge de travail de la fonction en diminuant le nombre de messages que les sondeurs d'événements peuvent échanger avec la fonction.

Mode alloué

Pour les charges de travail où vous devez optimiser le débit de votre mappage des sources d'événements, vous pouvez utiliser le mode provisionné. En mode provisionné, vous définissez des limites minimales et maximales pour le nombre de sondeurs d'événements alloués. Ces sondeurs d'événements alloués sont dédiés à votre mappage des sources d'événements et peuvent gérer les pics de messages inattendus grâce à une mise à l'échelle automatique réactive. Nous vous recommandons d'utiliser le mode provisionné pour les charges de travail Kafka soumises à des exigences de performance strictes.

Dans Lambda, un sondeur d'événements est une unité de calcul dont les capacités de débit varient selon le type de source d'événements. Pour Amazon MSK et Apache Kafka autogéré, chaque sondeur d'événements peut gérer jusqu'à 5 % MB/sec du débit ou jusqu'à 5 appels simultanés.

Par exemple, si la source de votre événement produit une charge utile moyenne de 1 Mo et que la durée moyenne de votre fonction est de 1 seconde, un seul sondeur d'événements Kafka peut prendre en charge 5 MB/sec débits et 5 appels Lambda simultanés (en supposant qu'il n'y ait aucune transformation de charge utile). Pour Amazon SQS, chaque sondeur d'événements peut gérer jusqu'à 1 % MB/sec du débit ou jusqu'à 10 appels simultanés. L'utilisation du mode provisionné entraîne des coûts supplémentaires en fonction de l'utilisation de votre sondeur d'événements. Pour plus d'informations sur la tarification, consultez Tarification AWS Lambda.

> **Note**
>
> Lorsque vous utilisez le mode provisionné, il n'est pas nécessaire de créer des points de terminaison AWS PrivateLink VPC ni d'accorder les autorisations associées dans le cadre de la configuration de votre réseau.

En mode provisionné, la plage de valeurs acceptées pour le nombre minimal de sondeurs d'événements (`MinimumPollers`) est comprise entre 1 et 200 inclus. La plage de valeurs acceptées pour le nombre maximal de sondeurs d'événements (`MaximumPollers`) est comprise entre 1 et 2 000 inclus. `MaximumPollers` doit être supérieur ou égal à `MinimumPollers`. En outre, pour maintenir un traitement ordonné au sein des partitions, Lambda limite le nombre de `MaximumPollers` au nombre de partitions dans la rubrique.

Pour plus de détails sur le choix des valeurs appropriées pour le nombre minimal et maximal de sondeurs d'événements, consultez Bonnes pratiques.

Vous pouvez configurer le mode provisionné pour le mappage des sources d'événements Kafka à l'aide de la console ou de l'API Lambda.

Pour configurer le mode provisionné pour un mappage des sources d'événements existant (console)

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez la fonction avec le mappage des sources d'événements pour laquelle vous souhaitez configurer le mode provisionné.
3. Choisissez Configuration, puis Déclencheurs.
4. Choisissez le mappage des sources d'événements pour lequel vous souhaitez configurer le mode alloué, puis choisissez Modifier.
5. Sous Mode provisionné, sélectionnez Configurer.

- Pour le Nombre minimal de sondeurs d'événements, saisissez une valeur comprise entre 1 et 200. Si vous ne spécifiez aucune valeur, Lambda choisit la valeur par défaut 1.
- Pour le Nombre maximal de sondeurs d'événements, saisissez une valeur comprise entre 1 et 2 000. Cette valeur doit être supérieure ou égale à la valeur du Nombre minimal de sondeurs d'événements. Si vous ne spécifiez aucune valeur, Lambda choisit la valeur par défaut 200.

6. Cliquez sur Enregistrer.

Vous pouvez configurer le mode provisionné par programmation à l'aide de l'ProvisionedPollerConfigobjet de votre. EventSourceMappingConfiguration Par exemple, la commande UpdateEventSourceMappingCLI suivante configure une `MinimumPollers` valeur de 5 et une `MaximumPollers` valeur de 100.

```
aws lambda update-event-source-mapping \
    --uuid a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
    --provisioned-poller-config '{"MinimumPollers": 5, "MaximumPollers": 100}'
```

Après avoir configuré le mode alloué, vous pouvez observer l'utilisation des sondeurs d'événements pour votre charge de travail en surveillant la métrique `ProvisionedPollers`. Pour plus d'informations, consultez the section called "Métriques de mappage des sources d'événements".

Pour désactiver le mode provisionné et revenir au mode par défaut (à la demande), vous pouvez utiliser la commande UpdateEventSourceMappingCLI suivante :

```
aws lambda update-event-source-mapping \
    --uuid a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
    --provisioned-poller-config '{}'
```

Fonctionnalités avancées de gestion des erreurs et de performance

Pour les mappages de sources d'événements Kafka avec le mode provisionné activé, vous pouvez configurer des fonctionnalités supplémentaires pour améliorer la gestion des erreurs et les performances :

- Configurations de nouvelles tentatives : contrôlez la façon dont Lambda gère les enregistrements ayant échoué avec un maximum de tentatives, des limites d'âge des enregistrements, un fractionnement par lots et des réponses partielles par lots.

- Destinations Kafka en cas de défaillance : envoyez les enregistrements ayant échoué vers une rubrique Kafka pour un traitement ou une analyse ultérieurs.

Bonnes pratiques et considérations lors de l'utilisation du mode provisionné

La configuration optimale du nombre minimal et maximal de sondeurs d'événements pour votre mappage des sources d'événements dépend des exigences de performances de votre application. Nous vous recommandons de commencer avec le nombre minimal de sondeurs d'événements par défaut afin de définir le profil de performances. Ajustez votre configuration en fonction des modèles de traitement des messages observés et du profil de performances souhaité.

Pour les charges de travail associées à des pics de trafic et à des exigences de performances strictes, augmentez le nombre minimal de sondeurs d'événements de manière à gérer les pics soudains de messages. Pour déterminer le nombre minimal de sondeurs d'événements requis, prenez en compte le nombre de messages par seconde de votre charge de travail et la taille moyenne des données utiles, et utilisez la capacité de débit d'un seul sondeur d'événements (jusqu'à 5 Mbit/s) comme référence.

Pour maintenir un traitement ordonné au sein d'une partition, Lambda limite le nombre maximal de sondeurs d'événements au nombre de partitions dans la rubrique. En outre, le nombre maximal de sondeurs d'événements auxquels votre mappage des sources d'événements peut être mis à l'échelle dépend des paramètres de simultanéité de la fonction.

Lorsque vous activez le mode provisionné, mettez à jour vos paramètres réseau pour supprimer les points de terminaison AWS PrivateLink VPC et les autorisations associées.

Optimisation des coûts pour le mode provisionné

Tarification du mode provisionné

Le mode provisionné est facturé en fonction du nombre minimum de sondeurs d'événements provisionnés et des sondeurs d'événements consommés lors du dimensionnement automatique. Les frais sont calculés à l'aide d'une unité de facturation appelée Event Poller Unit (EPU). Vous payez en fonction du nombre et de la durée des EPU utilisés, exprimés en Event-Poller-Unit-hours.

Vous pouvez utiliser le mode provisionné avec un seul ESM pour les applications sensibles aux performances ou vous pouvez regrouper plusieurs ESM au sein d'un même VPC afin de partager la capacité et les coûts de l'EPU. Les sections suivantes décrivent deux fonctionnalités qui vous aident à optimiser les coûts du mode provisionné. Pour plus de détails sur les tarifs, consultez la section Tarification AWS Lambda.

Utilisation améliorée de l'EPU

Chaque EPU prend en charge une capacité de MB/s débit allant jusqu'à 20 pour l'interrogation d'événements et prend en charge 10 sondeurs d'événements par défaut. Lorsque vous créez un mode provisionné pour Kafka ESM en définissant des sondeurs minimum et maximum, il utilise un nombre minimum d'interrogateurs pour approvisionner les EPU sur la base de 10 sondeurs d'événements par EPU par défaut. Cependant, chaque sondeur d'événements peut évoluer indépendamment pour prendre en charge jusqu'à 5 % de la capacité MB/s de débit, ce qui peut nécessiter une plus faible densité de sondeurs d'événements sur un EPU spécifique et peut déclencher le dimensionnement des EPU. Le nombre de sondeurs d'événements alloués sur un EPU dépend de la capacité de calcul consommée par chaque sondeur d'événements. Cette approche d'utilisation améliorée de l'EPU permet aux enquêteurs d'événements ayant des exigences de débit variables d'utiliser efficacement la capacité de l'EPU, réduisant ainsi les coûts pour tous les ESM.

Regroupement ESM

Pour optimiser davantage les coûts de votre mode provisionné, vous pouvez regrouper plusieurs eSM Kafka afin de partager la capacité de l'EPU. Grâce au regroupement ESM et à l'utilisation améliorée de l'EPU, vous pouvez réduire les coûts du mode provisionné jusqu'à 90 % pour les charges de travail à faible débit par rapport à l'exécution en mode ESM unique. Tous les ESM qui nécessitent moins d'une capacité EPU bénéficient du regroupement ESM. Ces ESM ont généralement besoin d'un minimum de sondeurs d'événements pour répondre à leurs besoins en matière de débit. Grâce à cette fonctionnalité, vous pouvez adopter le mode provisionné pour toutes vos charges de travail Kafka et bénéficier de fonctionnalités telles que la validation du schéma, le filtrage des Avro/Protobuf événements, les appels à faible latence et la gestion améliorée des erreurs, uniquement disponibles en mode provisionné.

Lorsque vous configurez le `PollerGroupName` paramètre avec la même valeur pour plusieurs eSM au sein d'un même Amazon VPC, ces derniers partagent les ressources EPU au lieu de nécessiter chacun une capacité EPU dédiée. Vous pouvez regrouper jusqu'à 100 ESM par groupe d'observateurs. Le nombre maximum d'observateurs agrégés pour tous les ESM d'un groupe ne peut pas dépasser 2 000.

Pour configurer le regroupement ESM (console)

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez votre fonction.
3. Choisissez Configuration, puis Déclencheurs.

4. Lorsque vous créez un nouveau mappage de source d'événements Kafka ou que vous modifiez un mappage existant, sélectionnez Configurer en mode provisionné.
5. Pour le Nombre minimal de sondeurs d’événements, saisissez une valeur comprise entre 1 et 200.
6. Pour le Nombre maximal de sondeurs d’événements, saisissez une valeur comprise entre 1 et 2 000.
7. Pour le nom du groupe Poller, entrez un identifiant pour le groupe. Utilisez le même nom pour les autres ESM que vous souhaitez regrouper.
8. Cliquez sur Enregistrer.

Pour configurer le regroupement ESM (AWS CLI)

L'exemple suivant crée un ESM avec un groupe de sondeurs nommé : `production-app-group`

```
aws lambda create-event-source-mapping \
  --function-name myFunction1 \
  --event-source-arn arn:aws:kafka:us-east-1:123456789012:cluster/MyCluster/abcd1234 \
  --topics topic1 \
  --starting-position LATEST \
  --provisioned-poller-config '{
    "MinimumPollers": 1,
    "MaximumPollers": 10,
    "PollerGroupName": "production-app-group"
  }'
```

Pour ajouter un autre ESM au même groupe (partageant la capacité de l'EPU), utilisez le même : PollerGroupName

```
aws lambda create-event-source-mapping \
  --function-name myFunction2 \
  --event-source-arn arn:aws:kafka:us-east-1:123456789012:cluster/MyCluster/abcd1234 \
  --topics topic2 \
  --starting-position LATEST \
  --provisioned-poller-config '{
    "MinimumPollers": 1,
    "MaximumPollers": 10,
    "PollerGroupName": "production-app-group"
  }'
```

> **Note**
>
> Vous pouvez mettre `PollerGroupName` à jour le pour déplacer un ESM vers un autre groupe, ou supprimer un ESM d'un groupe en transmettant une chaîne vide (« ») pour : `PollerGroupName`

```
# Move ESM to a different group
aws lambda update-event-source-mapping \
  --uuid a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
  --provisioned-poller-config '{
    "MinimumPollers": 1,
    "MaximumPollers": 10,
    "PollerGroupName": "new-group-name"
  }'

# Remove ESM from group (use dedicated resources)
aws lambda update-event-source-mapping \
  --uuid a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
  --provisioned-poller-config '{
    "MinimumPollers": 1,
    "MaximumPollers": 10,
    "PollerGroupName": ""
  }'
```

Considérations relatives aux stratégies de regroupement

- Limite des applications — Regroupez les ESM appartenant aux mêmes applications ou services pour une meilleure allocation et une meilleure gestion des coûts. Envisagez d'utiliser des conventions de dénomination telles que `app-name-environment` (par exemple,`order-processor-prod`).
- Schéma de trafic — Évitez de regrouper les ESM à haut débit et à trafic élevé, car cela pourrait entraîner une contention des ressources.
- Rayon d'explosion — Tenez compte de l'impact si l'infrastructure partagée rencontre des problèmes. Tous les ESM d'un même groupe sont concernés par les limites des ressources partagées. Pour les charges de travail critiques, vous pouvez utiliser des groupes distincts ou des ESM dédiés.

Exemple d'optimisation des coûts

Imaginons un scénario dans lequel vous disposez de 10 ESM, chacun étant configuré avec un sondeur d'événements et un débit inférieur à 2 : MB/s

Sans regroupement :

- Chaque ESM a besoin de son propre EPU
- Nombre total d'EPU nécessaires : 10
- Coût par EPU : 0$. 185/hour dans l'est des États-Unis (Virginie du Nord)
- Coût mensuel de l'EPU (720 heures) : 10 × 720 × 0,185$ = 1 332$

Avec regroupement :

- Les 10 ESM partagent la capacité de l'EPU
- 10 sondeurs événementiels peuvent être utilisés dans 1 EPU (avec 10 nouveaux sondeurs par support EPU)
- Nombre total d'EPU nécessaires : 1
- Coût mensuel de l'EPU (720 heures) : 1 × 720 × 0,185$ = 133,20$
- Économies de coûts : 90 % (1 198,80$ d'économies par mois)

Positions de départ des interrogations et flux Apache Kafka dans Lambda

Le StartingPosition paramètre indique à Lambda quand commencer à lire les messages provenant de votre flux Amazon MSK ou d'Apache Kafka autogéré. Vous avez le choix entre trois options :

- Dernier : Lambda commence à lire juste après l'enregistrement le plus récent de la rubrique Kafka.
- Supprimer l'horizon : Lambda commence par le dernier enregistrement non découpé de la rubrique Kafka. Il s'agit également de l'enregistrement le plus ancien de la rubrique.
- À l'horodatage : Lambda commence à lire à partir d'une position définie par un horodatage, en secondes Unix. Utilisez le StartingPositionTimestamp paramètre pour spécifier l'horodatage.

L'interrogation des flux lors des mises à jour et de la création du mappage des sources d'événements est finalement cohérente :

- Lors de la création du mappage des sources d'événements, le démarrage de l'interrogation des événements à partir du flux peut prendre plusieurs minutes.
- Lors des mises à jour du mappage des sources d'événements, l'arrêt et la reprise des événements d'interrogation depuis le flux peuvent prendre jusqu'à 90 secondes.

Ce comportement signifie que si vous spécifiez `LATEST` comme position de départ du flux, le mappage des sources d'événements peut manquer des événements lors d'une création ou d'une mise à jour. Pour vous assurer qu'aucun événement n'est manqué, spécifiez `TRIM_HORIZON` ou `AT_TIMESTAMP`.

Interroger les sujets de Kafka en mode file d'attente

Le mode file d'attente est un mode de consommation qui utilise des groupes de partage, qui est devenu disponible dans Apache Kafka 4.0 (le Kafka Queue Poller nécessite la version 4.2 ou ultérieure). Avec le mode File d'attente, vous pouvez traiter les messages thématiques de Kafka de manière non ordonnée et à haut débit à l'aide de groupes de partage. Contrairement aux groupes de consommateurs Kafka traditionnels qui attribuent des partitions exclusivement aux consommateurs, les groupes de partage permettent à plusieurs consommateurs de lire simultanément à partir des mêmes partitions. Cette méthode est similaire à celle utilisée par Amazon SQS pour traiter les messages provenant d'une file d'attente.

Lorsque vous créez un mappage de source d'événements pour un environnement autogéré Apache Kafka cluster, vous pouvez choisir entre deux modes de consommation :

- Diffusez (par défaut). Utilise les groupes de consommateurs Kafka avec un ordre par partition. Lambda attribue chaque partition à un seul consommateur.
- File d'attente. Utilise des groupes de partage, qui sont devenus disponibles dans Apache Kafka 4.0, pour un traitement à haut débit non ordonné (le Kafka Queue Poller nécessite la version 4.2 ou ultérieure). Avec les groupes de partage, plusieurs consommateurs peuvent lire simultanément à partir des mêmes partitions, de la même manière qu'Amazon SQS traite les messages d'une file d'attente.

Si vous ne spécifiez aucun mode de consommation, le mappage des sources d'événements utilise Stream. Cette page couvre le mode de consommation des files d'attente. Pour des informations générales sur l'utilisation de Lambda avec l'autogestion Apache Kafka, voir Utilisation de Lambda avec Apache Kafka autogéré.

En mode File d'attente, Lambda utilise le Kafka Share Consumer pour interroger les messages du sujet. Chaque sondeur d'événements traite les messages sur toutes les partitions sans ordre au niveau des partitions. Cela augmente la simultanéité pour chaque sondeur.

Configuration requise

Pour utiliser le mode de consommation des files d'attente, votre cluster Kafka doit répondre aux exigences suivantes :

- Apache Kafka version 4.2 ou ultérieure avec les groupes de partage activés. Kafka permet `share.version` par défaut, et vous pouvez le gérer via `kafka-features.sh`.

- Self-managed Apache Kafka Clusters (SMK) uniquement. Streaming géré par Amazon pour Apache Kafka (Amazon MSK) ne prend pas actuellement en charge le mode File d'attente. AWS ajoute le support MSK une fois que MSK propose Kafka 4.2 ou une version ultérieure avec les groupes de partage activés.

Comparaison des flux et des files d'attente

Fonctionnalité	Stream (par défaut)	File d’attente
Commander	Per-partition commande garantie	Aucune garantie de commande
Modèle de consommation	Groupe de consommateurs (cession exclusive de partage)	Groupe de partage (accès simultané aux partitions)
Débit par sondeur d'événements	Jusqu'à 5 MB/s	Jusqu'à 5 MB/s
Invocations simultanées par participant à l'événement	Jusqu’à 5	Jusqu’à 10
Modes de dimensionnement	On-demand et approvisionné	On-demand et approvisionné
Partage de l'EPU	Peut partager des EPU avec d'autres mappages de sources d'événements Kafka Streams	Isolé. Les mappages de sources d'événements de file d'attente ne sont partagés qu'avec d'autres mappages de sources d'événements de file d'attente
Cas d’utilisation	Traitement ordonné des événements	High-throughput charges de travail non ordonnées

Création d'un mappage de file

Pour créer un mappage de sources d'événements en mode file d'attente, définissez `ConsumptionMode` domaine de `SelfManagedKafkaEventSourceConfig` pour `Queue`. Dans les

exemples suivants, remplacez `my-function`, les points de terminaison du courtier, et `my-queue-topic` avec vos propres valeurs.

AWS INTERFACE DE LIGNE DE COMMANDE (CLI)

Les suivants AWS La commande CLI crée un mappage de source d'événements en mode file d'attente. Remplacer *my-function* avec le nom de votre fonction, le broker se termine par vos courtiers, et *my-queue-topic* avec votre sujet.

```
PROMPT> aws lambda create-event-source-mapping \
  --function-name my-function \
  --self-managed-event-source '{"Endpoints":{"KAFKA_BOOTSTRAP_SERVERS":["broker1.us-west-2.example.com:9092","broker2.us-west-2.example.com:9092"]}}' \
  --topics my-queue-topic \
  --batch-size 100 \
  --self-managed-kafka-event-source-config '{"ConsumptionMode": "Queue"}' \
  --provisioned-poller-config '{"MinimumPollers": 1, "MaximumPollers": 10}'
```

AWS CloudFormation

Les suivants AWS CloudFormation Le modèle crée un mappage de source d'événements en mode file d'attente. Remplacez les points de terminaison du courtier et *my-queue-topic* avec vos propres valeurs.

```
MyKafkaQueueESM:
  Type: AWS::Lambda::EventSourceMapping
  Properties:
    FunctionName: !Ref MyFunction
    SelfManagedEventSource:
      Endpoints:
        KafkaBootstrapServers:
          - broker1.us-west-2.example.com:9092
          - broker2.us-west-2.example.com:9092
    Topics:
      - my-queue-topic
    BatchSize: 100
    SelfManagedKafkaEventSourceConfig:
      ConsumptionMode: Queue
    ProvisionedPollerConfig:
      MinimumPollers: 1
      MaximumPollers: 10
```

Paramètres de configuration

Le tableau suivant répertorie les paramètres applicables aux mappages de sources d'événements en mode file d'attente.

Paramètre	Description	Plage/Par défaut
`BatchSize`	Nombre maximum d'enregis trements par lot envoyés à la fonction	1 à 10 000. Par défaut : 100
`Enabled`	Si le mappage des sources d'événements est actif	`true` ou `false`. Valeur par défaut : `true`
`FilterCriteria`	Modèles de filtrage des événements pour traiter uniquement les enregistr ements correspondants	Jusqu'à 5 modèles de filtre
`MaximumRetryAttempts`	Nombre maximum de tentative s pour les enregistrements ayant échoué	-1 à 10 000. Par défaut : 0 (en mode file d'attente, le broker Kafka effectue de nouvelles tentatives lorsqu'aucune destination en cas d'échec n'est configurée)
`BisectBatchOnFunct ionError`	Diviser le lot en deux en cas d'erreur de fonction	`true` ou `false`. Valeur par défaut : `false`
`ProvisionedPollerC onfig.MinimumPolle rs`	Nombre minimal de participa nts aux sondages d'événeme nts (mode provisionné)	1 à 200. Valeur par défaut : 1
`ProvisionedPollerC onfig.MaximumPolle rs`	Nombre maximum de personnes interrogées sur les événements (mode provision né)	1 à 2 000. Par défaut : 200

Paramètre	Description	Plage/Par défaut
`ProvisionedPollerConfig.PollerGroupName`	Nom du groupe pour le partage EPU (mode provisionné, mappages de sources d'événements en file d'attente uniquement)	String. Jusqu'à 100 mappages de sources d'événements par groupe
`SelfManagedKafkaEventSourceConfig.ConsumptionMode`	Mode de consommation pour la source de l'événement	Doit être `Queue` pour le mode file d'attente
`SchemaRegistryConfig`	Registre de schémas pour la validation des événements	Consultez Utilisation de registres de schémas avec les sources d'événements Kafka dans Lambda

Important

Le `MaximumBatchingWindowInSeconds` le paramètre est non pris en charge pour les mappages de sources d'événements en mode file d'attente. Le consommateur de Kafka Share utilise une reconnaissance explicite. Tous les enregistrements d'un lot doivent faire l'objet d'un accusé de réception explicite avant que le consommateur puisse en récupérer de nouveaux. Cela n'est pas compatible avec une fenêtre de traitement par lots basée sur le temps. Si vous spécifiez `MaximumBatchingWindowInSeconds` lors de la création d'un mappage de source d'événements en mode file d'attente, l'API renvoie une erreur de validation.

Fonctionnalités de mappage des sources d'événements prises en charge

Le tableau suivant répertorie les fonctionnalités de mappage des sources d'événements Lambda disponibles avec le mode Queue.

Fonctionnalité	Pris en charge	Remarques
Mode alloué	Oui	Configurez `MinimumPollers` et `MaximumPollers`
On-demand mode	Oui	Mode de mise à l'échelle par défaut. Lambda balance automatiquement les sondeurs jusqu'à 5 MB/s ou 50 appels simultanés, selon la première valeur atteinte. Aucune configuration supplémentaire n'est requise.
Filtrage des événements	Oui	Jusqu'à 5 modèles de filtre par mappage de source d'événement
Registre de schémas	Oui	Avro et Protobuf avec Glue Schema Registry ou Confluent Schema Registry. Le filtrage du registre des schémas n'est disponible qu'en mode provisionné.
Low-latency En traitement	Oui	Disponible en mode provisionné
Réessayez les configurations	Oui	`MaximumRetryAttempts` , `BisectBatchOnFunctionError`
On-failure destination (thème de Kafka)	Oui	Envoyer les enregistrements ayant échoué à un sujet Kafka
On-failure destination (SNS/SQS)	Oui	Envoyer les enregistrements ayant échoué à SNS ou SQS

Fonctionnalité	Pris en charge	Remarques
Enregistrement du mappage des sources d'événements	Oui	CloudWatch Journaux pour les diagnostics de mappage des sources d'événements
Groupement de mappages de sources d'événements (`PollerGroupName`)	Oui	Les mappages de sources d'événements en mode file d'attente peuvent partager des EPU avec d'autres mappages de sources d'événements en mode file d'attente uniquement (mode provisionné)
Fenêtre de traitement par lots	Non	Non pris en charge en raison du comportement du mode de blocage Share Consumer
Position de départ	Non	`StartingPosition` et `StartingPositionTimestamp` ne sont pas prises en charge. Le mode file d'attente lit toujours à partir de la position validée du groupe de partage.

Modes de dimensionnement

Les mappages de sources d'événements en mode file d'attente prennent en charge à la fois les modes de dimensionnement à la demande (par défaut) et provisionnés.

On-demand mode (par défaut)

En mode à la demande, Lambda gère automatiquement les sondeurs d'événements pour votre mappage des sources d'événements en mode file d'attente.

On-demand le mode permet d'effectuer jusqu'à 5 sondages d'événements par mappage de source d'événements. Il atteint son plafond à 5 MB/s débit global ou 50 appels simultanés (5 interrogateurs

multipliés par 10). Cela se produit quelle que soit la limite atteinte en premier. Pour dépasser ces limites, utilisez le mode provisionné. On-demand le mode ne nécessite aucune configuration supplémentaire au-delà des paramètres de mappage des sources d'événements standard.

Le tableau suivant répertorie les limites du mode à la demande.

Limite	Value
Débit par sondeur d'événements	Jusqu'à 1 MB/s
Invocations simultanées par participant à l'événement	Jusqu'à 10
Nombre maximum de participants à l'événement	5
Débit agrégé maximal	Jusqu'à 5 MB/s (5 personnes interrogées fois 1) MB/s)
Simultanéité agrégée maximale	Jusqu'à 50 invocations simultanées (5 sondeurs multipliés par 10)

Exemple — Mappage des sources d'événements en mode file d'attente en mode à la demande (AWS CLI)

Ce qui suit AWS La commande CLI crée un mappage de source d'événements en mode file d'attente en mode à la demande. Remplacer *my-function*, les points de terminaison du courtier, *my-queue-topic*, les ID de sous-réseau et l'ID du groupe de sécurité avec vos propres valeurs.

```
PROMPT> aws lambda create-event-source-mapping \
  --function-name my-function \
  --self-managed-event-source '{"Endpoints":{"KAFKA_BOOTSTRAP_SERVERS":["broker1.us-
west-2.example.com:9092","broker2.us-west-2.example.com:9092"]}}' \
  --topics my-queue-topic \
  --batch-size 100 \
  --self-managed-kafka-event-source-config '{"ConsumptionMode": "Queue"}' \
  --source-access-configurations
 '[{"Type":"VPC_SUBNET","URI":"subnet-0123456789abcdef0"},
{"Type":"VPC_SUBNET","URI":"subnet-0123456789abcdef1"},
{"Type":"VPC_SECURITY_GROUP","URI":"sg-0123456789abcdef0"}]'
```

Mode alloué

Pour les charges de travail soumises à des exigences de performances strictes ou à des modèles de trafic élevés, utilisez le mode provisionné. Le mode provisionné vous permet de contrôler directement le nombre minimum et maximum de sondeurs d'événements dédiés à votre mappage des sources d'événements en mode file d'attente.

Chaque sondeur d'événements en mode file d'attente en mode provisionné prend en charge jusqu'à 5 MB/s de débit et jusqu'à 10 appels Lambda simultanés.

Le tableau suivant répertorie les limites du mode provisionné.

Limite	Value
Débit par sondeur d'événements	Jusqu'à 5 MB/s
Invocations simultanées par participant à l'événement	Jusqu'à 10
Nombre minimum de participants à l'événement (`MinimumPollers`)	1 à 200. Valeur par défaut : 1
Nombre maximum de participants à l'événement (`MaximumPollers`)	1 à 2 000. Par défaut : 200
Mappages des sources d'événements par groupe de sondeurs	Jusqu'à 100
Nombre maximum total de personnes interrogées par groupe de sondeurs	2 000
Débit par EPU (agrégé)	Jusqu'à 5 MB/s par poller ; l'agrégat dépend de la densité de remplissage du poller

Le mode provisionné est facturé en fonction de l'utilisation de l'Event Poller Unit (EPU). Pour plus d'informations sur la tarification, consultez la page AWS Lambda Pricing (Tarification).

Exemple — Mappage de sources d'événements en mode file d'attente avec le mode provisionné (AWS CLI)

Ce qui suit AWS La commande CLI crée un mappage de source d'événements en mode file d'attente en mode provisionné.

```
PROMPT> aws lambda create-event-source-mapping \
  --function-name my-function \
  --self-managed-event-source '{"Endpoints":{"KAFKA_BOOTSTRAP_SERVERS":["broker1.us-
west-2.example.com:9092","broker2.us-west-2.example.com:9092"]}}' \
  --topics my-queue-topic \
  --batch-size 100 \
  --self-managed-kafka-event-source-config '{"ConsumptionMode": "Queue"}' \
  --provisioned-poller-config '{"MinimumPollers": 5, "MaximumPollers": 100}' \
  --source-access-configurations
 '[{"Type":"VPC_SUBNET","URI":"subnet-0123456789abcdef0"},
{"Type":"VPC_SUBNET","URI":"subnet-0123456789abcdef1"},
{"Type":"VPC_SECURITY_GROUP","URI":"sg-0123456789abcdef0"}]'
```

Remplacez les espaces réservés suivants par vos propres valeurs :

- *subnet-0123456789abcdef0* et *subnet-0123456789abcdef1*: vos identifiants de sous-réseau.
- *sg-0123456789abcdef0*: l'identifiant de votre groupe de sécurité.
- `MinimumPollers` et `MaximumPollers`: paramétré en fonction de vos besoins en matière de débit.

> **Note**
>
> Pour passer du mode provisionné au mode à la demande, passez un champ vide `ProvisionedPollerConfig`:
>
> ```
> PROMPT> aws lambda update-event-source-mapping \
>   --uuid a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
>   --provisioned-poller-config '{}'
> ```

Sélection du mode de dimensionnement

Considération	On-demand	Alloué
Configuration	Aucune configuration supplémentaire	Configurez `MinimumPollers` et `MaximumPollers`
Coût	Pas de frais EPU supplémentaires	Frais EPU basés sur l'utilisation par heure
Idéal pour	Low-concurrency charges de travail	Exigences de latence strictes, trafic élevé
Groupement de mappages de sources d'événements (`PollerGroupName`)	Non pris en charge	Pris en charge. Partagez des EPU entre les mappages de sources d'événements de la file d'attente
Low-latency En traitement	Non disponible	Available
Filtrage du registre des schémas (Avro/Protobuf)	Non disponible	Available

EPU partageant l'isolation

En mode provisionné, vous pouvez regrouper plusieurs mappages de sources d'événements au sein du même VPC afin de partager la capacité de l'Event Poller Unit (EPU) en leur attribuant la même capacité `PollerGroupName`. Le regroupement de mappages de sources d'événements permet de regrouper des mappages de sources d'événements à faible débit sur des EPU partagés au lieu de nécessiter chacun une capacité dédiée, ce qui réduit les coûts du mode provisionné. Pour plus de détails, consultez Optimisation des coûts pour le mode provisionné.

Les mappages de sources d'événements en mode file d'attente ne partagent les EPU qu'avec d'autres mappages de sources d'événements en mode file d'attente. UNE `PollerGroupName` utilisé par un mappage de source d'événements en mode Queue ne peut pas être partagé avec un mappage de source d'événements Kafka Streams, et vice versa. Si vous configurez un `PollerGroupName` déjà utilisé par l'autre mode de consommation, `CreateEventSourceMapping`

renvoie une erreur de validation. Pour utiliser le regroupement de mappages de sources d'événements avec le mode File d'attente, créez un `PollerGroupName` dédié à vos mappages de sources d'événements de file d'attente.

Exemple d’évènement

Lorsque Lambda appelle votre fonction avec une source d'événements en mode Queue, la charge utile de l'événement est identique à celle d'un événement Kafka standard. Chaque enregistrement inclut le sujet, la partition, le décalage, l'horodatage, ainsi que la clé et la valeur codées en base64 :

```
{
  "eventSource": "SelfManagedKafka",
  "bootstrapServers": "broker1.example.com:9092,broker2.example.com:9092",
  "records": {
    "my-queue-topic-0": [
      {
        "topic": "my-queue-topic",
        "partition": 0,
        "offset": 15,
        "timestamp": 1545084650987,
        "timestampType": "CREATE_TIME",
        "key": "abcDEFghiJKLmnoPQRstuVWXyz1234==",
        "value": "SGVsbG8sIHRoaXMgaXMgYSB0ZXN0Lg==",
        "headers": [
          {
            "headerKey": [104, 101, 97, 100, 101, 114, 86, 97, 108, 117, 101]
          }
        ]
      }
    ],
    "my-queue-topic-3": [
      {
        "topic": "my-queue-topic",
        "partition": 3,
        "offset": 42,
        "timestamp": 1545084651000,
        "timestampType": "CREATE_TIME",
        "key": "YW5vdGhlcktleQ==",
        "value": "VGhpcyBpcyBhbm90aGVyIG1lc3NhZ2U=",
        "headers": []
      }
    ]
  }
```

```
}
```

> **Idempotence requise**
>
> Les mappages de sources d'événements Lambda traitent chaque événement au moins une fois, ce qui peut entraîner un traitement dupliqué des enregistrements. Le mode Queue ne garantissant pas l'ordre, le traitement des doublons ou des erreurs de traitement peut produire des résultats incorrects, tels qu'un double comptage ou un état incohérent, si le code de votre fonction n'est pas idempotent. Rendez votre code de fonction idempotent.

Limitations

- Self-managed Clusters Kafka uniquement. Amazon MSK n'est pas pris en charge au lancement.
- Apache Kafka 4.2 ou version ultérieure requise. Le cluster doit prendre en charge le protocole Share Consumer avec les groupes de partage activés.
- La fenêtre de traitement par lots n'est pas prise en charge. Le `MaximumBatchingWindowInSeconds` Le paramètre ne peut pas être utilisé avec les mappages de sources d'événements Kafka Queue.
- Position de départ non prise en charge. `StartingPosition` et `StartingPositionTimestamp` ne peut pas être utilisé avec les mappages de sources d'événements en mode file d'attente. Le groupe d'actions consomme à partir de sa position de compensation engagée.
- Isolation EPU. Les mappages de sources d'événements en mode file d'attente ne peuvent pas partager les EPU avec les mappages de sources d'événements de Kafka Streams. Utiliser séparément `PollerGroupName` valeurs.

ID de groupe de consommateurs personnalisable dans Lambda

Lorsque vous configurez Amazon MSK ou Apache Kafka autogéré comme source d'événements, vous pouvez spécifier un ID de groupe de consommateurs. Cet ID de groupe de consommateurs est un identifiant existant pour le groupe de consommateurs Kafka auquel vous souhaitez que votre fonction d'événement Lambda rejoigne. Vous pouvez utiliser cette fonction pour migrer facilement toutes les configurations de traitement d'enregistrements Kafka en cours depuis d'autres clients vers Lambda.

Kafka distribue les messages à tous les consommateurs d'un groupe de consommateurs. Si vous spécifiez un ID de groupe de consommateurs qui compte d'autres consommateurs actifs, Lambda ne reçoit qu'une partie des messages de la rubrique Kafka. Si vous souhaitez que Lambda gère tous les messages de la rubrique, désactivez tous les autres consommateurs de ce groupe de consommateurs.

De plus, si vous spécifiez un identifiant de groupe de consommateurs et que Kafka trouve un groupe de consommateurs valide portant le même identifiant, Lambda ignore le mappage de StartingPositionla source de votre événement. Lambda commence plutôt à traiter les enregistrements en fonction de la compensation engagée par le groupe de consommateurs. Si vous spécifiez un identifiant de groupe de consommateurs et que Kafka ne trouve aucun groupe de consommateurs existant, Lambda configure votre source d'événement avec le `StartingPosition` spécifié.

L'identifiant du groupe de consommateurs que vous spécifiez doit être unique parmi toutes vos sources d'événements Kafka. Après avoir créé un mappage des sources d'événements Kafka avec l'identifiant de groupe de consommateurs spécifié, vous ne pouvez plus mettre à jour cette valeur.

Filtrage des événements provenant d'Amazon MSK et sources d'événements Apache Kafka autogéré

Vous pouvez utiliser le filtrage des événements pour contrôler les enregistrements d'un flux ou d'une file d'attente que Lambda envoie à votre fonction d'événement. Pour obtenir des informations générales sur le fonctionnement du filtrage des événements, consultez the section called "Filtrage des événements".

> **Note**
>
> Les mappages Amazon MSK et Apache Kafka autogéré ne prennent en charge que le filtrage sur la clé `value`.

Rubriques

- Notions de base du filtrage d'événements Lambda

Notions de base du filtrage d'événements Lambda

Supposons qu'un producteur écrive des messages à une rubrique de votre cluster Kafka, au format JSON valide ou sous forme de chaînes simples. Un exemple d'enregistrement ressemblerait à ce qui suit, avec le message converti en chaîne encodée en Base64 dans le champ `value`.

```
{
    "mytopic-0":[
        {
            "topic":"mytopic",
            "partition":0,
            "offset":15,
            "timestamp":1545084650987,
            "timestampType":"CREATE_TIME",
            "value":"SGVsbG8sIHRoaXMgaXMgYSB0ZXN0Lg==",
            "headers":[]
        }
    ]
}
```

Supposons que votre producteur Apache Kafka écrive des messages dans votre rubrique au format JSON suivant.

```
{
    "device_ID": "AB1234",
    "session":{
        "start_time": "yyyy-mm-ddThh:mm:ss",
        "duration": 162
    }
}
```

Vous pouvez utiliser la clé `value` pour filtrer les enregistrements. Supposons que vous vouliez filtrer uniquement les enregistrements où `device_ID` commence par les lettres AB. L'objet `FilterCriteria` serait le suivant.

```
{
    "Filters": [
        {
            "Pattern": "{ \"value\" : { \"device_ID\" : [ { \"prefix\": \"AB\" } ] } }"
        }
    ]
}
```

Pour plus de clarté, voici la valeur du `Pattern` de filtre étendu en JSON simple :

```
{
    "value": {
        "device_ID": [ { "prefix": "AB" } ]
      }
}
```

Vous pouvez ajouter votre filtre à l'aide de la console AWS CLI ou d'un AWS SAM modèle.

Console

Pour ajouter ce filtre à l'aide de la console, suivez les instructions de Attacher des critères de filtre à un mappage de sources d'événements (console) et saisissez la chaîne suivante comme critère de filtre.

```
{ "value" : { "device_ID" : [ { "prefix":  "AB" } ] } }
```

AWS CLI

Pour créer un nouveau mappage de source d'événements avec ces critères de filtre à l'aide de AWS Command Line Interface (AWS CLI), exécutez la commande suivante.

```
aws lambda create-event-source-mapping \
    --function-name my-function \
    --event-source-arn arn:aws:kafka:us-east-2:123456789012:cluster/my-cluster/
b-8ac7cc01-5898-482d-be2f-a6b596050ea8 \
    --filter-criteria '{"Filters": [{"Pattern": "{ \"value\" : { \"device_ID\" :
 [ { \"prefix\":  \"AB\" } ] } }"}]}'
```

Pour ajouter ces critères de filtre à un mappage des sources d'événements existant, exécutez la commande suivante.

```
aws lambda update-event-source-mapping \
    --uuid "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE" \
    --filter-criteria '{"Filters": [{"Pattern": "{ \"value\" : { \"device_ID\" :
 [ { \"prefix\":  \"AB\" } ] } }"}]}'
```

AWS SAM

Pour ajouter ce filtre à l'aide de AWS SAM, ajoutez l'extrait suivant au modèle YAML de votre source d'événement.

```
FilterCriteria:
  Filters:
    - Pattern: '{ "value" : { "device_ID" : [ { "prefix":  "AB" } ] } }'
```

Avec Kafka, vous pouvez également filtrer les enregistrements dont le message est une chaîne simple. Supposons que vous vouliez ignorer les messages dont la chaîne est « error ». L'objet `FilterCriteria` se présente comme suit.

```
{
    "Filters": [
        {
            "Pattern": "{ \"value\" : [ { \"anything-but\": [ \"error\" ] } ] }"
        }
    ]
```

```
}
```

Pour plus de clarté, voici la valeur du `Pattern` de filtre étendu en JSON simple :

```
{
    "value": [
        {
        "anything-but": [ "error" ]
        }
    ]
}
```

Vous pouvez ajouter votre filtre à l'aide de la console AWS CLI ou d'un AWS SAM modèle.

Console

Pour ajouter ce filtre à l'aide de la console, suivez les instructions de Attacher des critères de filtre à un mappage de sources d'événements (console) et saisissez la chaîne suivante comme critère de filtre.

```
{ "value" : [ { "anything-but": [ "error" ] } ] }
```

AWS CLI

Pour créer un nouveau mappage de source d'événements avec ces critères de filtre à l'aide de AWS Command Line Interface (AWS CLI), exécutez la commande suivante.

```
aws lambda create-event-source-mapping \
    --function-name my-function \
    --event-source-arn arn:aws:kafka:us-east-2:123456789012:cluster/my-cluster/
b-8ac7cc01-5898-482d-be2f-a6b596050ea8 \
    --filter-criteria '{"Filters": [{"Pattern": "{ \"value\" : [ { \"anything-but\":
 [ \"error\" ] } ] }"}]}'
```

Pour ajouter ces critères de filtre à un mappage des sources d'événements existant, exécutez la commande suivante.

```
aws lambda update-event-source-mapping \
    --uuid "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE" \
    --filter-criteria '{"Filters": [{"Pattern": "{ \"value\" : [ { \"anything-but\":
 [ \"error\" ] } ] }"}]}'
```

AWS SAM

Pour ajouter ce filtre à l'aide de AWS SAM, ajoutez l'extrait suivant au modèle YAML de votre source d'événement.

```
FilterCriteria:
  Filters:
    - Pattern: '{ "value" : [ { "anything-but": [ "error" ] } ] }'
```

Les messages Kafka doivent être des chaînes UTF-8 codées, soit des chaînes simples, soit au format JSON. C'est parce que Lambda décode les tableaux d'octets de Kafka avant d'appliquer les critères de filtrage. UTF-8 Si vos messages utilisent un autre encodage, tel que UTF-16 l'ASCII, ou si le format du message ne correspond pas au format, Lambda traite uniquement les `FilterCriteria` filtres de métadonnées. Le tableau suivant résume le comportement spécifique :

Format du du message entrant	Modèle de filtre de format pour les propriétés des messages	Action obtenue.
Chaîne de texte brut	Chaîne de texte brut	Lambda filtre en fonction de vos critères de filtre.
Chaîne de texte brut	Pas de modèle de filtre pour les propriétés des données	Lambda filtre (uniquement selon les autres propriétés de métadonnées) en fonction de vos critères de filtre.
Chaîne de texte brut	JSON valide	Lambda filtre (uniquement selon les autres propriétés de métadonnées) en fonction de vos critères de filtre.
JSON valide	Chaîne de texte brut	Lambda filtre (uniquement selon les autres propriétés de métadonnées) en fonction de vos critères de filtre.
JSON valide	Pas de modèle de filtre pour les propriétés des données	Lambda filtre (uniquement selon les autres propriétés de

Format du du message entrant	Modèle de filtre de format pour les propriétés des messages	Action obtenue.
		métadonnées) en fonction de vos critères de filtre.
JSON valide	JSON valide	Lambda filtre en fonction de vos critères de filtre.
Non-UTF-8 chaîne codée	JSON, chaîne de texte brut ou aucun modèle	Lambda filtre (uniquement selon les autres propriétés de métadonnées) en fonction de vos critères de filtre.

Utilisation de registres de schémas avec les sources d’événements Kafka dans Lambda

Les registres de schémas vous aident à définir et gérer des schémas de flux de données. Un schéma définit la structure et le format d'un enregistrement de données. Dans le contexte des mappages de sources d'événements Kafka, vous pouvez configurer un registre de schémas pour valider la structure et le format des messages Kafka par rapport à des schémas prédéfinis avant qu'ils n'atteignent votre fonction d'événement Lambda. Cela ajoute une couche de gouvernance des données à votre application et vous pouvez gérer efficacement les formats de données, garantir la conformité des schémas et optimiser les coûts grâce au filtrage des événements.

Cette fonctionnalité est compatible avec tous les langages de programmation, mais tenez compte des points importants suivants :

- Powertools for Lambda fournit un support spécifique pour Java, Python TypeScript et assure la cohérence avec les modèles de développement Kafka existants et permet un accès direct aux objets métier sans code de désérialisation personnalisé
- Cette fonctionnalité n’est disponible que pour les mappages des sources d’événements utilisant le mode provisionné. Le registre des schémas ne prend pas en charge les mappages des sources d’événements en mode à la demande. Si vous utilisez le mode provisionné et qu’un registre de schéma est configuré, vous ne pouvez pas passer en mode à la demande, sauf si vous supprimez d’abord la configuration de votre registre de schémas. Pour plus d’informations, consultez the section called “Mode alloué”
- Vous ne pouvez configurer qu’un seul registre de schémas par mappage des sources d’événements (ESM). L'utilisation d'un registre de schémas avec votre source d'événements Kafka peut augmenter votre utilisation de l'unité Lambda Event Poller (EPU), ce qui constitue une dimension tarifaire pour le mode provisionné.

Rubriques

- Options du registre de schémas
- Comment Lambda effectue la validation du schéma pour les messages Kafka
- Configuration d’un registre de schémas Kafka
- Filtrage pour Avro et Protobuf
- Formats de données utiles et comportement de désérialisation
- Utilisation de données désérialisées dans les fonctions d'événement Lambda

- Méthodes d'authentification pour votre registre de schémas
- Gestion des erreurs et résolution des problèmes liés au registre de schémas

Options du registre de schémas

Lambda prend en charge les options de registre de schémas suivantes :

- AWS Glue Registre des schémas
- Registre de schémas Confluent Cloud
- Self-managed Registre des schémas Confluent

Votre registre de schémas prend en charge la validation des messages dans les formats de données suivants :

- Apache Avro
- Protocol Buffers (Protobuf)
- Schéma JSON (JSON-SE)

Pour utiliser un registre de schémas, assurez-vous d'abord que votre mappage des sources d'événements est en mode provisionné. Lorsque vous utilisez un registre de schémas, Lambda ajoute des métadonnées relatives au schéma aux données utiles. Pour plus d'informations, consultez Formats de données utiles et comportement de désérialisation.

Comment Lambda effectue la validation du schéma pour les messages Kafka

Lorsque vous configurez un registre de schémas, Lambda exécute les étapes suivantes pour chaque message Kafka :

1. Lambda interroge l'enregistrement Kafka de votre cluster.
2. Lambda valide les attributs de message sélectionnés dans l'enregistrement par rapport à un schéma spécifique de votre registre de schémas.
   - Si le schéma associé au message n'est pas trouvé dans le registre, Lambda envoie le message à une DLQ avec le code de motif `SCHEMA_NOT_FOUND`.
3. Lambda désérialise le message conformément à la configuration du registre de schémas pour valider le message. Si le filtrage des événements est configuré, Lambda effectue ensuite le filtrage en fonction des critères de filtre configurés.

- Si la désérialisation échoue, Lambda envoie le message à une DLQ avec le code de motif `DESERIALIZATION_ERROR`. Si aucune DLQ n'est configurée, Lambda abandonne le message.

4. Si le message est validé par le registre de schémas et qu'il n'est pas filtré selon vos critères de filtre, Lambda invoque votre fonction avec le message.

Cette fonctionnalité est destinée à valider les messages déjà produits à l'aide de clients Kafka intégrés à un registre de schémas. Nous vous recommandons de configurer vos producteurs Kafka pour qu'ils fonctionnent avec votre registre de schémas afin de créer des messages correctement formatés.

Configuration d'un registre de schémas Kafka

Les étapes de console suivantes ajoutent une configuration de registre de schémas Kafka à votre mappage des sources d'événements.

Ajouter une configuration de registre de schémas Kafka à votre mappage des sources d'événements (console)

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez Configuration.
3. Choisissez Déclencheurs.
4. Sélectionnez le mappage des sources d'événements Kafka pour lequel vous souhaitez configurer un registre de schémas, puis choisissez Modifier.
5. Sous Configuration du sondeur d'événements, choisissez Configurer le registre de schémas. Votre mappage des sources d'événements doit être en mode provisionné pour voir cette option.
6. Pour l'URI du registre de schéma, entrez l'ARN de votre registre de AWS Glue schémas ou l'URL HTTPS de votre registre de schémas Confluent Cloud ou de votre registre de schémas Self-Managed Confluent.
7. Les étapes de configuration suivantes indiquent à Lambda comment accéder à votre registre de schémas. Pour plus d'informations, consultez ???.

   - Pour Type de configuration d'accès, choisissez le type d'authentification utilisé par Lambda pour accéder à votre registre de schémas.
   - Pour URI de configuration d'accès, entrez l'ARN du secret Secrets Manager pour vous authentifier auprès de votre registre de schémas, le cas échéant. Assurez-vous que le rôle d'exécution de votre fonction contient les autorisations appropriées.

8. Le champ Chiffrement s'applique uniquement si votre registre de schémas est signé par une autorité de certification (CA) privée ou une autorité de certification (CA) qui ne figure pas dans le magasin d'approbations Lambda. Le cas échéant, fournissez la clé secrète contenant le certificat CA privé utilisé par votre registre de schémas pour le chiffrement TLS.
9. Pour Format d'enregistrement de l'événement, choisissez la manière dont vous souhaitez que Lambda transmette les enregistrements à votre fonction après la validation du schéma. Pour plus d'informations consultez Exemples de formats de données utiles.
   - Si vous choisissez JSON, Lambda fournit les attributs que vous sélectionnez dans Attribut de validation du schéma ci-dessous au format JSON standard. Pour les attributs que vous ne sélectionnez pas, Lambda les fournit en l'état.
   - Si vous choisissez SOURCE, Lambda fournit les attributs que vous avez sélectionnés dans Attribut de validation du schéma ci-dessous dans leur format source d'origine.
10. Pour Attribut de validation du schéma, sélectionnez les attributs de message que Lambda doit valider et désérialiser à l'aide de votre registre de schémas. Vous devez sélectionner au moins une option entre KEY et VALUE. Si vous avez choisi JSON pour le format d'enregistrement d'événement, Lambda désérialise également les attributs de message sélectionnés avant de les envoyer à votre fonction. Pour plus d'informations, consultez Formats de données utiles et comportement de désérialisation.
11. Cliquez sur Enregistrer.

Vous pouvez également utiliser l'API Lambda pour créer ou mettre à jour votre mappage des sources d'événements avec une configuration de registre de schémas. Les exemples suivants montrent comment configurer un registre de schéma AWS Glue ou un registre de schéma Confluent à l'aide du AWS CLI, qui correspond aux opérations d'CreateEventSourceMappingAPI UpdateEventSourceMappinget de la référence AWS Lambda d'API :

> **Important**
>
> Si vous mettez à jour un champ de configuration du registre de schéma à l'aide de l'`update-event-source-mapping`API AWS CLI ou de l'API, vous devez mettre à jour tous les champs de configuration du registre de schéma.

Create Event Source Mapping

```
aws lambda create-event-source-mapping \
```

```
  --function-name my-schema-validator-function \
  --event-source-arn arn:aws:kafka:us-east-1:123456789012:cluster/my-cluster/
a1b2c3d4-5678-90ab-cdef-11111EXAMPLE \
  --topics my-kafka-topic \
  --provisioned-poller-config MinimumPollers=1,MaximumPollers=1 \
  --amazon-managed-kafka-event-source-mapping '{
      "SchemaRegistryConfig" : {
          "SchemaRegistryURI": "https://abcd-ef123.us-west-2.aws.confluent.cloud",
          "AccessConfigs": [{
              "Type": "BASIC_AUTH",
              "URI": "arn:aws:secretsmanager:us-
east-1:123456789012:secret:secretName"
          }],
          "EventRecordFormat": "JSON",
          "SchemaValidationConfigs": [
          {
              "Attribute": "KEY"
          },
          {
              "Attribute": "VALUE"
          }]
      }
  }'
```

Update AWS Glue Schema Registry

```
aws lambda update-event-source-mapping \
    --uuid a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
    --amazon-managed-kafka-event-source-mapping '{
        "SchemaRegistryConfig" : {
            "SchemaRegistryURI": "arn:aws:glue:us-east-1:123456789012:registry/
registryName",
            "EventRecordFormat": "JSON",
            "SchemaValidationConfigs": [
            {
                "Attribute": "KEY"
            },
            {
                "Attribute": "VALUE"
            }]
        }
    }'
```

Update Confluent Schema Registry with Authentication

```
aws lambda update-event-source-mapping \
    --uuid a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
    --amazon-managed-kafka-event-source-mapping '{
        "SchemaRegistryConfig" : {
            "SchemaRegistryURI": "https://abcd-ef123.us-west-2.aws.confluent.cloud",
            "AccessConfigs": [{
                "Type": "BASIC_AUTH",
                "URI": "arn:aws:secretsmanager:us-
east-1:123456789012:secret:secretName"
            }],
            "EventRecordFormat": "JSON",
            "SchemaValidationConfigs": [
            {
                "Attribute": "KEY"
            },
            {
                "Attribute": "VALUE"
            }]
        }
    }'
```

Update Confluent Schema Registry without Authentication

```
aws lambda update-event-source-mapping \
    --uuid a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
    --amazon-managed-kafka-event-source-mapping '{
        "SchemaRegistryConfig" : {
            "SchemaRegistryURI": "https://abcd-ef123.us-west-2.aws.confluent.cloud",
            "EventRecordFormat": "JSON",
            "SchemaValidationConfigs": [
            {
                "Attribute": "KEY"
            },
            {
                "Attribute": "VALUE"
            }]
        }
    }'
```

Remove Schema Registry Configuration

Pour supprimer une configuration de registre de schéma de votre mappage de source d'événements, vous pouvez utiliser la commande CLI UpdateEventSourceMappingdans la référence AWS Lambda d'API.

```
aws lambda update-event-source-mapping \
    --uuid a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
    --amazon-managed-kafka-event-source-mapping '{
        "SchemaRegistryConfig" : {}
    }'
```

Filtrage pour Avro et Protobuf

Lorsque vous utilisez les formats Avro ou Protobuf avec un registre de schémas, vous pouvez appliquer un filtrage d'événements à votre fonction d'événement Lambda. Les modèles de filtre sont appliqués à la représentation JSON classique désérialisée de vos données après validation du schéma. Par exemple, avec un schéma Avro définissant les détails du produit, y compris le prix, vous pouvez filtrer les messages en fonction de la valeur du prix :

> **Note**
>
> Lors de la désérialisation, l'objet Avro est converti en JSON standard, ce qui signifie qu'il ne peut pas être reconverti directement en objet Avro. Si vous devez effectuer une conversion en objet Avro, utilisez plutôt le format SOURCE.
> Pour la désérialisation de Protobuf, les noms de champs dans le JSON obtenu correspondent à ceux définis dans votre schéma, plutôt que d'être convertis en casse mixte comme le fait généralement Protobuf. Gardez cela à l'esprit lorsque vous créez des schémas de filtrage.

```
aws lambda create-event-source-mapping \
    --function-name myAvroFunction \
    --topics myAvroTopic \
    --starting-position TRIM_HORIZON \
    --kafka-bootstrap-servers '["broker1:9092", "broker2:9092"]' \
    --schema-registry-config '{
        "SchemaRegistryURI": "arn:aws:glue:us-east-1:123456789012:registry/
myAvroRegistry",
        "EventRecordFormat": "JSON",
```

```
        "SchemaValidationConfigs": [
            {
                "Attribute": "VALUE"
            }
        ]
    }' \
    --filter-criteria '{
        "Filters": [
            {
                "Pattern": "{ \"value\" : { \"field_1\" : [\"value1\"], \"field_2\" :
[\"value2\"] } }"
            }
        ]
    }'
```

Dans cet exemple, le modèle de filtre analyse l'objet `value` en faisant correspondre les messages dans `field_1` avec `"value1"`, et `field_2` avec `"value2"`. Les critères de filtre sont évalués par rapport aux données désérialisées, une fois que Lambda a converti le message du format Avro en JSON.

Pour plus d'informations sur le filtrage des événements, consultez la section Filtrage des événements Lambda.

Formats de données utiles et comportement de désérialisation

Lorsque vous utilisez un registre de schémas, Lambda fournit les données utiles finales à votre fonction dans un format similaire aux données utiles d'événement ordinaires, avec quelques champs supplémentaires. Les champs supplémentaires dépendent du paramètre `SchemaValidationConfigs`. Pour chaque attribut que vous sélectionnez pour validation (clé ou valeur), Lambda ajoute les métadonnées de schéma correspondantes aux données utiles.

> **Note**
>
> Vous devez mettre à jour vos aws-lambda-java-events vers la version 3.16.0 ou supérieure pour utiliser les champs de métadonnées du schéma.

Par exemple, si vous validez le champ `value`, Lambda ajoute un champ appelé `valueSchemaMetadata` à vos données utiles. De même, pour le champ `key`, Lambda ajoute un champ appelé `keySchemaMetadata`. Ces métadonnées contiennent des informations sur le format des données et l'ID de schéma utilisés pour la validation :

```
"valueSchemaMetadata": {
    "dataFormat": "AVRO",
    "schemaId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

Le paramètre `EventRecordFormat` peut être défini sur `JSON` ou `SOURCE`, ce qui détermine la manière dont Lambda gère les données validées par le schéma avant de les transmettre à votre fonction. Chaque option offre des capacités de traitement différentes :

- `JSON` : Lambda désérialise les attributs validés au format JSON standard, ce qui rend les données prêtes à être utilisées directement dans les langages prenant en charge le format JSON natif. Ce format est idéal lorsque vous n'avez pas besoin de conserver le format binaire d'origine ou de travailler avec les classes générées.
- `SOURCE`- Lambda préserve le format binaire original des données sous forme de Base64-encoded chaîne, ce qui permet une conversion directe en objets Avro ou Protobuf. Ce format est essentiel lorsque vous travaillez avec des langages fortement typés ou lorsque vous devez conserver toutes les fonctionnalités des schémas Avro ou Protobuf.

Sur la base de ces caractéristiques de format et des considérations spécifiques au langage, nous recommandons les formats suivants :

Formats recommandés selon le langage de programmation

Language	Avro	Protobuf	JSON
Java	SOURCE	SOURCE	SOURCE
Python	JSON	JSON	JSON
NodeJS	JSON	JSON	JSON
.NET	SOURCE	SOURCE	SOURCE
Autres	JSON	JSON	JSON

Les sections suivantes décrivent ces formats en détail et fournissent des exemples de données utiles pour chaque format.

Format JSON

Si vous choisissez `JSON` comme tel`EventRecordFormat`, Lambda valide et désérialise les attributs de message que vous avez sélectionnés dans le `SchemaValidationConfigs` champ (les attributs). `key` and/or `value` Lambda fournit ces attributs sélectionnés sous forme de chaînes codées en Base64 de leur représentation JSON standard dans votre fonction.

> **Note**
>
> Lors de la désérialisation, l'objet Avro est converti en JSON standard, ce qui signifie qu'il ne peut pas être reconverti directement en objet Avro. Si vous devez effectuer une conversion en objet Avro, utilisez plutôt le format SOURCE.
> Pour la désérialisation de Protobuf, les noms de champs dans le JSON obtenu correspondent à ceux définis dans votre schéma, plutôt que d'être convertis en casse mixte comme le fait généralement Protobuf. Gardez cela à l'esprit lorsque vous créez des schémas de filtrage.

Voici un exemple de données utiles, en supposant que vous choisissez `JSON` comme `EventRecordFormat` et les attributs `key` et `value` comme `SchemaValidationConfigs` :

```
{
   "eventSource":"aws:kafka",
   "eventSourceArn":"arn:aws:kafka:us-east-1:123456789012:cluster/vpc-2priv-2pub/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111-1",
   "bootstrapServers":"b-2.demo-cluster-1.a1bcde.c1.kafka.us-
east-1.amazonaws.com:9092,b-1.demo-cluster-1.a1bcde.c1.kafka.us-
east-1.amazonaws.com:9092",
   "records":{
      "mytopic-0":[
         {
            "topic":"mytopic",
            "partition":0,
            "offset":15,
            "timestamp":1545084650987,
            "timestampType":"CREATE_TIME",
            "key":"abcDEFghiJKLmnoPQRstuVWXyz1234==", //Base64 encoded string of JSON
            "keySchemaMetadata": {
                "dataFormat": "AVRO",
                "schemaId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
            },
            "value":"abcDEFghiJKLmnoPQRstuVWXyz1234", //Base64 encoded string of JSON
```

```
            "valueSchemaMetadata": {
                "dataFormat": "AVRO",
                "schemaId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
            },
            "headers":[
               {
                  "headerKey":[
                     104,
                     101,
                     97,
                     100,
                     101,
                     114,
                     86,
                     97,
                     108,
                     117,
                     101
                  ]
               }
            ]
         }
      ]
   }
}
```

Dans cet exemple :

- `key` et `value` sont des chaînes codées en Base64 de leur représentation JSON après désérialisation.
- Lambda inclut des métadonnées de schéma pour les deux attributs dans `keySchemaMetadata` et `valueSchemaMetadata`.
- Votre fonction peut décoder les chaînes `key` et `value` pour accéder aux données JSON désérialisées.

Le format JSON est recommandé pour les langages qui ne sont pas fortement typés, tels que Python ou Node.js. Ces langages offrent la prise en charge native de la conversion de JSON en objets.

Format source

Si vous choisissez SOURCE comme EventRecordFormat, Lambda valide toujours l'enregistrement par rapport au registre de schémas, mais fournit les données binaires d'origine à votre fonction sans désérialisation. Ces données binaires sont fournies sous la forme d'une chaîne codée en Base64 des données d'octets d'origine, les métadonnées ajoutées par le producteur étant supprimées. Par conséquent, vous pouvez directement convertir les données binaires brutes en objets Avro et Protobuf dans le code de votre fonction. Nous vous recommandons d'utiliser Powertools for AWS Lambda, qui désérialise les données binaires brutes et vous fournit directement les objets Avro et Protobuf.

Par exemple, si vous configurez Lambda pour valider à la fois les attributs key et value, mais que vous utilisez le format SOURCE, votre fonction reçoit des données utiles semblables à celles-ci :

```
{
    "eventSource": "aws:kafka",
    "eventSourceArn": "arn:aws:kafka:us-east-1:123456789012:cluster/vpc-2priv-2pub/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111-1",
    "bootstrapServers": "b-2.demo-cluster-1.a1bcde.c1.kafka.us-
east-1.amazonaws.com:9092,b-1.demo-cluster-1.a1bcde.c1.kafka.us-
east-1.amazonaws.com:9092",
    "records": {
        "mytopic-0": [
            {
                "topic": "mytopic",
                "partition": 0,
                "offset": 15,
                "timestamp": 1545084650987,
                "timestampType": "CREATE_TIME",
                "key": "abcDEFghiJKLmnoPQRstuVWXyz1234==", // Base64 encoded string of
 Original byte data, producer-appended metadata removed
                "keySchemaMetadata": {
                    "dataFormat": "AVRO",
                    "schemaId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
                },
                "value": "abcDEFghiJKLmnoPQRstuVWXyz1234==", // Base64 encoded string
 of Original byte data, producer-appended metadata removed
                "valueSchemaMetadata": {
                    "dataFormat": "AVRO",
                    "schemaId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
                },
                "headers": [
```

```
                    {
                        "headerKey": [
                            104,
                            101,
                            97,
                            100,
                            101,
                            114,
                            86,
                            97,
                            108,
                            117,
                            101
                        ]
                    }
                ]
            }
        ]
    }
}
```

Dans cet exemple :

- `key` et `value` contiennent tous deux les données binaires d'origine sous forme de chaînes codées en Base64.
- Votre fonction doit gérer la désérialisation à l'aide des bibliothèques appropriées.

Il `EventRecordFormat` est recommandé de choisir `SOURCE` pour si vous utilisez Protobuf-generated des objets Avro-generated ou, en particulier avec des fonctions Java. Cela est dû au fait que Java est fortement typé et nécessite des désérialiseurs spécifiques pour les formats Avro et Protobuf. Dans le code de votre fonction, vous pouvez utiliser votre bibliothèque Avro ou Protobuf préférée pour désérialiser les données.

Utilisation de données désérialisées dans les fonctions d'événement Lambda

Powertools for vous AWS Lambda aide à désérialiser les enregistrements Kafka dans votre code de fonction en fonction du format que vous utilisez. Cet utilitaire simplifie l'utilisation des enregistrements Kafka en gérant la conversion des données et en fournissant des objets prêts à l'emploi.

Pour utiliser Powertools AWS Lambda dans votre fonction, vous devez ajouter Powertools en tant que couche AWS Lambda ou en tant que dépendance lors de la création de votre fonction

d'événement Lambda. Pour obtenir des instructions de configuration et plus d'informations, consultez les Powertools pour obtenir AWS Lambda la documentation correspondant à votre langue préférée :

- Powertools pour AWS Lambda (Java)
- Powertools pour AWS Lambda (Python)
- Outils électriques pour AWS Lambda () TypeScript
- Powertools pour AWS Lambda (.NET)

> **Note**
>
> Lorsque vous travaillez avec l'intégration du registre de schémas, vous pouvez choisir le format `SOURCE` ou `JSON`. Chaque option prend en charge différents formats de sérialisation, comme indiqué ci-dessous :
>
> | Format | Prend en charge |
> | --- | --- |
> | SOURCE | Avro et Protobuf (en utilisant l'intégration du registre de schémas Lambda) |
> | JSON | Données JSON |

Lorsque vous utilisez le `JSON` format `SOURCE` or, vous pouvez utiliser Powertools pour vous aider AWS à désérialiser les données de votre code de fonction. Voici des exemples de gestion de différents formats de données :

AVRO

Exemple Java :

```
package org.demo.kafka;

import org.apache.kafka.clients.consumer.ConsumerRecord;
import org.apache.kafka.clients.consumer.ConsumerRecords;
import org.demo.kafka.avro.AvroProduct;
import org.slf4j.Logger;
import org.slf4j.LoggerFactory;
```

```
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;

import software.amazon.lambda.powertools.kafka.Deserialization;
import software.amazon.lambda.powertools.kafka.DeserializationType;
import software.amazon.lambda.powertools.logging.Logging;

public class AvroDeserializationFunction implements
 RequestHandler<ConsumerRecords<String, AvroProduct>, String> {

    private static final Logger LOGGER =
 LoggerFactory.getLogger(AvroDeserializationFunction.class);

    @Override
    @Logging
    @Deserialization(type = DeserializationType.KAFKA_AVRO)
    public String handleRequest(ConsumerRecords<String, AvroProduct> records,
 Context context) {
        for (ConsumerRecord<String, AvroProduct> consumerRecord : records) {
            LOGGER.info("ConsumerRecord: {}", consumerRecord);

            AvroProduct product = consumerRecord.value();
            LOGGER.info("AvroProduct: {}", product);

            String key = consumerRecord.key();
            LOGGER.info("Key: {}", key);
        }

        return "OK";
    }

}
```

Exemple Python :

```
from aws_lambda_powertools.utilities.kafka_consumer.kafka_consumer import
 kafka_consumer
from aws_lambda_powertools.utilities.kafka_consumer.schema_config import
 SchemaConfig
from aws_lambda_powertools.utilities.kafka_consumer.consumer_records import
 ConsumerRecords

from aws_lambda_powertools.utilities.typing import LambdaContext
```

```
from aws_lambda_powertools import Logger

logger = Logger(service="kafkaConsumerPowertools")

value_schema_str = open("customer_profile.avsc", "r").read()

schema_config = SchemaConfig(
value_schema_type="AVRO",
value_schema=value_schema_str)

@kafka_consumer(schema_config=schema_config)
def lambda_handler(event: ConsumerRecords, context:LambdaContext):

  for record in event.records:
      value = record.value
      logger.info(f"Received value: {value}")
```

TypeScript exemple :

```
import { kafkaConsumer } from '@aws-lambda-powertools/kafka';

import type { ConsumerRecords } from '@aws-lambda-powertools/kafka/types';
import { Logger } from '@aws-lambda-powertools/logger';
import type { Context } from 'aws-lambda';

const logger = new Logger();

type Value = {
    id: number;
    name: string;
    price: number;
};

const schema = '{
    "type": "record",
    "name": "Product",
    "fields": [
        { "name": "id", "type": "int" },
        { "name": "name", "type": "string" },
        { "name": "price", "type": "double" }
    ]
}';
```

```
export const handler = kafkaConsumer<string, Value>(
    (event: ConsumerRecords<string, Value>, _context: Context) => {
        for (const record of event.records) {
            logger.info(Processing record with key: ${record.key});
            logger.info(Record value: ${JSON.stringify(record.value)});
            // You can add more processing logic here
        }
    },
    {
        value: {
            type: 'avro',
            schema: schema,
        },
    }
);
```

Exemple .NET :

```
using Amazon.Lambda.Core;
using AWS.Lambda.Powertools.Kafka;
using AWS.Lambda.Powertools.Kafka.Avro;
using AWS.Lambda.Powertools.Logging;
using Com.Example;

// Assembly attribute to enable the Lambda Event Function's Kafka event to be
 converted into a .NET class.
[assembly: LambdaSerializer(typeof(PowertoolsKafkaAvroSerializer))]

namespace ProtoBufClassLibrary;

public class Function
{
    public string FunctionHandler(ConsumerRecords<string, CustomerProfile> records,
 ILambdaContext context)
    {
        foreach (var record in records)
        {
            Logger.LogInformation("Processing messagem from topic: {topic}",
 record.Topic);
            Logger.LogInformation("Partition: {partition}, Offset: {offset}",
 record.Partition, record.Offset);
            Logger.LogInformation("Produced at: {timestamp}", record.Timestamp);
```

```
            foreach (var header in record.Headers.DecodedValues())
            {
                Logger.LogInformation($"{header.Key}: {header.Value}");
            }

            Logger.LogInformation("Processing order for: {fullName}",
 record.Value.FullName);
        }

        return "Processed " + records.Count() + " records";
    }
}
```

PROTOBUF

Exemple Java :

```
package org.demo.kafka;

import org.apache.kafka.clients.consumer.ConsumerRecord;
import org.apache.kafka.clients.consumer.ConsumerRecords;
import org.demo.kafka.protobuf.ProtobufProduct;
import org.slf4j.Logger;
import org.slf4j.LoggerFactory;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;

import software.amazon.lambda.powertools.kafka.Deserialization;
import software.amazon.lambda.powertools.kafka.DeserializationType;
import software.amazon.lambda.powertools.logging.Logging;

public class ProtobufDeserializationFunction
        implements RequestHandler<ConsumerRecords<String, ProtobufProduct>, String>
 {

    private static final Logger LOGGER =
 LoggerFactory.getLogger(ProtobufDeserializationFunction.class);

    @Override
    @Logging
    @Deserialization(type = DeserializationType.KAFKA_PROTOBUF)
    public String handleRequest(ConsumerRecords<String, ProtobufProduct> records,
 Context context) {
```

```
        for (ConsumerRecord<String, ProtobufProduct> consumerRecord : records) {
            LOGGER.info("ConsumerRecord: {}", consumerRecord);

            ProtobufProduct product = consumerRecord.value();
            LOGGER.info("ProtobufProduct: {}", product);

            String key = consumerRecord.key();
            LOGGER.info("Key: {}", key);
        }

        return "OK";
    }

}
```

Exemple Python :

```
from aws_lambda_powertools.utilities.kafka_consumer.kafka_consumer import
 kafka_consumer

from aws_lambda_powertools.utilities.kafka_consumer.schema_config import
 SchemaConfig
from aws_lambda_powertools.utilities.kafka_consumer.consumer_records import
 ConsumerRecords

from aws_lambda_powertools.utilities.typing import LambdaContext
from aws_lambda_powertools import Logger

from user_pb2 import User # protobuf generated class

logger = Logger(service="kafkaConsumerPowertools")

schema_config = SchemaConfig(
value_schema_type="PROTOBUF",
value_schema=User)

@kafka_consumer(schema_config=schema_config)
def lambda_handler(event: ConsumerRecords, context:LambdaContext):

  for record in event.records:
      value = record.value
      logger.info(f"Received value: {value}")
```

TypeScript exemple :

```
import { kafkaConsumer } from '@aws-lambda-powertools/kafka';
import type { ConsumerRecords } from '@aws-lambda-powertools/kafka/types';
import { Logger } from '@aws-lambda-powertools/logger';
import type { Context } from 'aws-lambda';
import { Product } from './product.generated.js';

const logger = new Logger();

type Value = {
    id: number;
    name: string;
    price: number;
};

export const handler = kafkaConsumer<string, Value>(
    (event: ConsumerRecords<string, Value>, _context: Context) => {
        for (const record of event.records) {
            logger.info(Processing record with key: ${record.key});
            logger.info(Record value: ${JSON.stringify(record.value)});
        }
    },
    {
        value: {
            type: 'protobuf',
            schema: Product,
        },
    }
);
```

Exemple .NET :

```
using Amazon.Lambda.Core;
using AWS.Lambda.Powertools.Kafka;
using AWS.Lambda.Powertools.Kafka.Protobuf;
using AWS.Lambda.Powertools.Logging;
using Com.Example;

// Assembly attribute to enable the Lambda function's Kafka event to be converted
 into a .NET class.
[assembly: LambdaSerializer(typeof(PowertoolsKafkaProtobufSerializer))]
```

```
namespace ProtoBufClassLibrary;

public class Function
{
    public string FunctionHandler(ConsumerRecords<string, CustomerProfile> records,
 ILambdaContext context)
    {
        foreach (var record in records)
        {
            Logger.LogInformation("Processing messagem from topic: {topic}",
 record.Topic);
            Logger.LogInformation("Partition: {partition}, Offset: {offset}",
 record.Partition, record.Offset);
            Logger.LogInformation("Produced at: {timestamp}", record.Timestamp);

            foreach (var header in record.Headers.DecodedValues())
            {
                Logger.LogInformation($"{header.Key}: {header.Value}");
            }

            Logger.LogInformation("Processing order for: {fullName}",
 record.Value.FullName);
        }

        return "Processed " + records.Count() + " records";
    }
}
```

JSON

Exemple Java :

```
package org.demo.kafka;

import org.apache.kafka.clients.consumer.ConsumerRecord;
import org.apache.kafka.clients.consumer.ConsumerRecords;
import org.slf4j.Logger;
import org.slf4j.LoggerFactory;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;

import software.amazon.lambda.powertools.kafka.Deserialization;
import software.amazon.lambda.powertools.kafka.DeserializationType;
```

```
import software.amazon.lambda.powertools.logging.Logging;

public class JsonDeserializationFunction implements
 RequestHandler<ConsumerRecords<String, Product>, String> {

    private static final Logger LOGGER =
 LoggerFactory.getLogger(JsonDeserializationFunction.class);

    @Override
    @Logging
    @Deserialization(type = DeserializationType.KAFKA_JSON)
    public String handleRequest(ConsumerRecords<String, Product> consumerRecords,
 Context context) {
        for (ConsumerRecord<String, Product> consumerRecord : consumerRecords) {
            LOGGER.info("ConsumerRecord: {}", consumerRecord);

            Product product = consumerRecord.value();
            LOGGER.info("Product: {}", product);

            String key = consumerRecord.key();
            LOGGER.info("Key: {}", key);
        }

        return "OK";
    }
}
```

Exemple Python :

```
from aws_lambda_powertools.utilities.kafka_consumer.kafka_consumer import
 kafka_consumer

from aws_lambda_powertools.utilities.kafka_consumer.schema_config import
 SchemaConfig
from aws_lambda_powertools.utilities.kafka_consumer.consumer_records import
 ConsumerRecords

from aws_lambda_powertools.utilities.typing import LambdaContext
from aws_lambda_powertools import Logger

logger = Logger(service="kafkaConsumerPowertools")

schema_config = SchemaConfig(value_schema_type="JSON")
```

```
@kafka_consumer(schema_config=schema_config)
def lambda_handler(event: ConsumerRecords, context:LambdaContext):

  for record in event.records:
      value = record.value
      logger.info(f"Received value: {value}")
```

TypeScript exemple :

```
import { kafkaConsumer } from '@aws-lambda-powertools/kafka';
import type { ConsumerRecords } from '@aws-lambda-powertools/kafka/types';
import { Logger } from '@aws-lambda-powertools/logger';
import type { Context } from 'aws-lambda';

const logger = new Logger();

type Value = {
    id: number;
    name: string;
    price: number;
};

export const handler = kafkaConsumer<string, Value>(
    (event: ConsumerRecords<string, Value>, _context: Context) => {
        for (const record of event.records) {
            logger.info(Processing record with key: ${record.key});
            logger.info(Record value: ${JSON.stringify(record.value)});
            // You can add more processing logic here
        }
    },
    {
        value: {
            type: 'json',
        },
    }
);
```

Exemple .NET :

```
using Amazon.Lambda.Core;
using AWS.Lambda.Powertools.Kafka;
using AWS.Lambda.Powertools.Kafka.Json;
```

```
using AWS.Lambda.Powertools.Logging;
using Com.Example;

// Assembly attribute to enable the Lambda function's Kafka event to be converted
 into a .NET class.
[assembly: LambdaSerializer(typeof(PowertoolsKafkaJsonSerializer))]

namespace JsonClassLibrary;

public class Function
{
    public string FunctionHandler(ConsumerRecords<string, CustomerProfile> records,
 ILambdaContext context)
    {
        foreach (var record in records)
        {
            Logger.LogInformation("Processing messagem from topic: {topic}",
 record.Topic);
            Logger.LogInformation("Partition: {partition}, Offset: {offset}",
 record.Partition, record.Offset);
            Logger.LogInformation("Produced at: {timestamp}", record.Timestamp);

            foreach (var header in record.Headers.DecodedValues())
            {
                Logger.LogInformation($"{header.Key}: {header.Value}");
            }

            Logger.LogInformation("Processing order for: {fullName}",
 record.Value.FullName);
        }

        return "Processed " + records.Count() + " records";
    }
}
```

Méthodes d’authentification pour votre registre de schémas

Pour utiliser un registre de schémas, Lambda doit pouvoir y accéder de façon sécurisée. Si vous travaillez avec un registre de AWS Glue schémas, Lambda s'appuie sur l'authentification IAM. Cela signifie que le rôle d'exécution de votre fonction doit disposer des autorisations suivantes pour accéder au AWS Glue registre :

- GetRegistrydans la référence de l'API AWS Glue Web
- GetSchemaVersiondans la référence de l'API AWS Glue Web

Exemple de politique IAM requise :

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "glue:GetRegistry",
                "glue:GetSchemaVersion"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

> **Note**
>
> Pour les registres de AWS Glue schéma, si vous fournissez `AccessConfigs` un AWS Glue registre, Lambda renvoie une exception de validation.

Si vous travaillez avec un registre de schémas Confluent, vous pouvez choisir l'une des quatre méthodes d'authentification prises en charge pour le `Type` paramètre de votre KafkaSchemaRegistryAccessConfigobjet :

- BASIC_AUTH : Lambda utilise le nom d'utilisateur et le mot de passe ou l'authentification par clé d'API et secret d'API pour accéder à votre registre. Si vous choisissez cette option, indiquez l'ARN Secrets Manager contenant vos informations d'identification dans le champ URI.
- CLIENT_CERTIFICATE_TLS_AUTH : Lambda utilise l'authentification TLS mutuelle avec les certificats clients. Pour utiliser cette option, Lambda doit avoir accès à la fois au certificat et à la clé

privée. Indiquez l'ARN Secrets Manager contenant ces informations d'identification dans le champ URI.

- OAUTHBEARER_AUTH — Lambda demande un jeton d'accès à votre fournisseur d'identité OAuth 2.0 et l'envoie à votre registre en tant que jeton porteur. Lambda actualise le jeton avant son expiration. Si vous choisissez cette option, indiquez l'ARN du Gestionnaire de Secrets contenant votre secret OAuth dans le champ URI. Le secret utilise les mêmes champs que le secret pour l'authentification du courtier et prend en charge les deux mêmes types de subvention. Pour le contenu du secret, voirthe section called "Configuration du secret OAuth".
- NO_AUTH : le certificat CA public doit être signé par une autorité de certification située dans le magasin d'approbations Lambda. Pour un CA/self-signed certificat privé, vous configurez le certificat CA racine du serveur. Pour utiliser cette option, omettez le paramètre `AccessConfigs`.

En outre, si Lambda a besoin d'accéder à un certificat CA privé pour vérifier le certificat TLS de votre registre de schémas, choisissez `SERVER_ROOT_CA_CERT` comme `Type` et fournissez l'ARN Secrets Manager au certificat dans le champ URI.

> **Note**
>
> Pour configurer l'option `SERVER_ROOT_CA_CERT` dans la console, fournissez l'ARN secret contenant le certificat dans le champ Chiffrement.

La configuration d'authentification de votre registre de schémas est distincte de toute authentification que vous avez configurée pour votre cluster Kafka. Vous devez configurer les deux séparément, même s'ils utilisent des méthodes d'authentification similaires.

Gestion des erreurs et résolution des problèmes liés au registre de schémas

Lorsque vous utilisez un registre de schémas avec votre source d'événements Amazon MSK, vous pouvez rencontrer diverses erreurs. Cette section fournit des conseils sur les problèmes courants et leur résolution.

Erreurs de configuration

Ces erreurs se produisent lors de la configuration de votre registre de schémas.

Mode provisionné requis

Message d'erreur : `SchemaRegistryConfig is only available for Provisioned Mode. To configure Schema Registry, please enable Provisioned Mode by specifying MinimumPollers in ProvisionedPollerConfig.`

Résolution : activez le mode provisionné pour votre mappage des sources d'événements en configurant le paramètre `MinimumPollers` dans `ProvisionedPollerConfig`.

URL de registre de schémas non valide

Message d'erreur : `Malformed SchemaRegistryURI provided. Please provide a valid URI or ARN. For example, https://schema-registry.example.com:8081 or arn:aws:glue:us-east-1:123456789012:registry/ExampleRegistry.`

Solution : Fournissez une URL HTTPS valide pour le registre des schémas Confluent ou un ARN valide pour le registre des AWS Glue schémas.

Format d'enregistrement d'événement non valide ou manquant

Message d'erreur : `EventRecordFormat is a required field for SchemaRegistryConfig. Please provide one of supported format types: SOURCE, JSON.`

Résolution : Spécifiez SOURCE ou JSON EventRecordFormat dans la configuration de votre registre de schéma.

Attributs de validation en double

Message d'erreur : `Duplicate KEY/VALUE Attribute in SchemaValidationConfigs. SchemaValidationConfigs must contain at most one KEY/VALUE Attribute.`

Résolution : Supprimez les attributs KEY ou VALUE dupliqués de votre SchemaValidationConfigs. Chaque type d'attribut ne peut apparaître qu'une seule fois.

Configuration de validation manquante

Message d'erreur : `SchemaValidationConfigs is a required field for SchemaRegistryConfig.`

Solution : Ajoutez SchemaValidationConfigs à votre configuration en spécifiant au moins un attribut de validation (KEY ou VALUE).

Erreurs d’accès et d’autorisation

Ces erreurs se produisent lorsque Lambda ne peut pas accéder au registre de schémas en raison de problèmes d’autorisation ou d’authentification.

AWS Glue Accès au registre du schéma refusé

- Message d’erreur : `Cannot access Glue Schema with provided role. Please ensure the provided role can perform the GetRegistry and GetSchemaVersion Actions on your schema.`
- Résolution : ajoutez les autorisations requises (`glue:GetRegistry` et `glue:GetSchemaVersion`) au rôle d’exécution de votre fonction.

Accès au registre de schémas Confluent refusé

- Message d’erreur : `Cannot access Confluent Schema with the provided access configuration.`
- Solution : vérifiez que vos informations d’authentification (stockées dans Secrets Manager) sont correctes et que vous disposez des autorisations nécessaires pour accéder au registre de schémas.

Cross-account AWS Glue Registre des schémas

- Message d’erreur : `Cross-account Glue Schema Registry ARN not supported.`
- Solution : utilisez un registre de AWS Glue schémas enregistré dans le même AWS compte que votre fonction d'événement Lambda.

Cross-region AWS Glue Registre des schémas

- Message d’erreur : `Cross-region Glue Schema Registry ARN not supported.`
- Solution : utilisez un registre de AWS Glue schémas situé dans la même région que votre fonction d'événement Lambda.

Problèmes d’accès au secret

- Message d’erreur : `Lambda received InvalidRequestException from Secrets Manager.`
- Solution : Vérifiez que le rôle d'exécution de votre fonction est autorisé à accéder au secret et que celui-ci n'est pas chiffré avec une AWS KMS clé par défaut si vous y accédez depuis un autre compte.

Erreurs de connexion

Ces erreurs se produisent lorsque Lambda ne parvient pas à établir une connexion au registre de schémas.

Problèmes de connectivité VPC

- Message d'erreur : `Cannot connect to your Schema Registry. Your Kafka cluster's VPC must be able to connect to the schema registry. You can provide access by configuring AWS PrivateLink or a NAT Gateway or VPC Peering between Kafka Cluster VPC and the schema registry VPC.`
- Solution : configurez votre réseau VPC pour autoriser les connexions au registre de schéma à l'aide AWS PrivateLink d'une passerelle NAT ou d'un peering VPC.

Échec d'établissement d'une liaison TLS

- Message d'erreur : `Unable to establish TLS handshake with the schema registry. Please provide correct CA-certificate or client certificate using Secrets Manager to access your schema registry.`
- Solution : vérifiez que vos certificats CA et vos certificats clients (pour mTLS) sont corrects et bien configurés dans Secrets Manager.

étranglement

- Message d'erreur : `Receiving throttling errors when accessing the schema registry. Please increase API TPS limits for your schema registry.`
- Résolution : augmentez les limites de débit d'API pour votre registre de schémas ou réduisez le taux de demandes provenant de votre application.

Self-managed erreurs de registre de schéma

- Message d'erreur : `Lambda received an internal server an unexpected error from the provided self-managed schema registry.`
- Solution : vérifiez l'état et la configuration de votre serveur de registre de schémas autogéré.

Traitement à faible latence pour les sources d’événements Kafka

AWS Lambda prend en charge de manière native le traitement des événements à faible latence pour les applications qui nécessitent des latences constantes de bout en bout inférieures à 100 millisecondes. Cette page fournit des informations de configuration et des recommandations pour permettre des flux de travail à faible latence.

Activer le traitement à faible latence

Pour activer le traitement à faible latence sur un mappage des sources d’événements Kafka, la configuration de base suivante est requise :

- Activez le mode provisionné. Pour plus d’informations, consultez Mode alloué.
- Définissez le paramètre du mappage des sources d’événements `MaximumBatchingWindowInSeconds` sur 0. Pour plus d’informations, consultez Comportement de traitement par lots.

Fine-tuning votre Kafka ESM à faible latence

Tenez compte des recommandations suivantes pour optimiser votre mappage des sources d’événements Kafka pour une faible latence :

Configuration du mode provisionné

En mode provisionné pour le mappage des sources d'événements Kafka, vous pouvez affiner le débit de votre mappage des sources d'événements en configurant un nombre minimum et maximum de ressources appelées sondages d'événements. Un sondeur d'événements (ou un interrogateur) représente une ressource de calcul qui sous-tend le mappage d'une source d'événements en mode provisionné et alloue jusqu'à 5 % de débit. MB/s Chaque sondeur d’événements prend en charge jusqu’à 5 invocations Lambda simultanées.

Pour déterminer la configuration optimale de sondeurs pour votre application, tenez compte de votre taux d’ingestion maximal et de vos exigences de traitement. Étudions un exemple simplifié :

Avec une taille de lot de 20 enregistrements et une durée cible moyenne de la fonction d'événement de 50 ms, chaque sondeur peut traiter 2 000 enregistrements par seconde, dans la limite de 5 MB/s . Ceci est calculé comme suit : (20 enregistrements × 1000ms/50ms) × 5 appels Lambda simultanés. Par conséquent, si le taux d’ingestion maximal souhaité est de 20 000 enregistrements par seconde, vous aurez besoin d’au moins 10 sondeurs d’événements.

> **Note**
>
> Nous vous recommandons de prévoir des sondeurs d'événements supplémentaires en tant que tampon de sûreté afin d'éviter de fonctionner constamment à pleine capacité.

Le mode provisionné met à l'échelle vos sondeurs d'événements automatiquement en fonction des modèles de trafic dans les limites minimales et maximales de sondeurs d'événements configurées, ce qui peut déclencher un rééquilibrage, et par conséquent introduire une latence supplémentaire. Vous pouvez désactiver l'autoscaling en configurant la même valeur pour le nombre minimal et maximal de sondeurs d'événements.

Considérations supplémentaires

Voici quelques considérations supplémentaires :

- Les démarrages à froid à partir de l'invocation de votre fonction cible Lambda peuvent augmenter la latence de bout en bout. Pour réduire ce risque, pensez à activer la simultanéité provisionnée ou à activer SnapStartla fonction cible du mappage des sources d'événements. En outre, optimisez l'allocation de mémoire de votre fonction pour garantir des exécutions cohérentes et optimales.
- Lorsqu'il `MaximumBatchingWindowInSeconds` est défini sur 0, Lambda traite immédiatement tous les enregistrements disponibles sans attendre de remplir la taille complète du lot. Par exemple, si la taille de votre lot est définie sur 1 000 enregistrements mais que seuls 100 enregistrements sont disponibles, Lambda traite ces 100 enregistrements immédiatement plutôt que d'attendre que les 1 000 enregistrements complets soient accumulés.

> **Important**
>
> La configuration optimale pour un traitement à faible latence varie considérablement selon votre charge de travail spécifique. Nous vous recommandons vivement de tester différentes configurations avec votre charge de travail réelle afin de déterminer les meilleurs paramètres pour votre cas d'utilisation.

Configuration des contrôles de gestion des erreurs pour les sources d'événements Kafka

Vous pouvez configurer la façon dont Lambda gère les erreurs et les nouvelles tentatives pour vos mappages de sources d'événements Kafka. Ces configurations vous aident à contrôler la manière dont Lambda traite les enregistrements ayant échoué et gère le comportement des nouvelles tentatives.

Configurations de nouvelle tentative disponibles

Les configurations de nouvelle tentative suivantes sont disponibles pour Amazon MSK et les sources d'événements Kafka autogérées :

- Nombre maximal de tentatives : nombre maximal de tentatives de Lambda lorsque votre fonction événementielle renvoie une erreur. Cela ne compte pas la tentative d'invocation initiale. La valeur par défaut est -1 (infini). Lorsque vous configurez à la fois un nombre infini de tentatives et une destination en cas d'échec, Lambda applique automatiquement un maximum de 10 tentatives.
- Age maximum d'enregistrement : âge maximum d'un enregistrement que Lambda envoie à votre fonction. La valeur par défaut est -1 (infini).
- Fractionner le lot en cas d'erreur : lorsque votre fonction renvoie une erreur, divisez le lot en deux lots plus petits et réessayez chacun séparément. Cela permet d'isoler les enregistrements problématiques.
- Réponse partielle par lot : autorisez votre fonction à renvoyer des informations sur les enregistrements d'un lot dont le traitement a échoué, afin que Lambda puisse réessayer uniquement les enregistrements ayant échoué.

Configuration des contrôles de gestion des erreurs (console)

Vous pouvez configurer le comportement des nouvelles tentatives lors de la création ou de la mise à jour d'un mappage de source d'événements Kafka dans la console Lambda.

Pour configurer le comportement des nouvelles tentatives pour une source d'événements Kafka (console)

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez le nom de votre fonction.
3. Effectuez l’une des actions suivantes :

- Pour ajouter un nouveau déclencheur Kafka, sous Vue d'ensemble des fonctions, choisissez Ajouter un déclencheur.
- Pour modifier un déclencheur Kafka existant, choisissez-le, puis choisissez Modifier.

4. Sous Configuration du sondeur d'événements, sélectionnez le mode provisionné pour configurer les contrôles de gestion des erreurs :

   a. Pour Réessayer, entrez le nombre maximum de tentatives (0 à 10 000, ou -1 pour un nombre infini).
   b. Pour Age maximum d'enregistrement, entrez l'âge maximum en secondes (60-604800, ou -1 pour un nombre infini).
   c. Pour activer le fractionnement par lots en cas d'erreur, sélectionnez Fractionner le lot en cas d'erreur.
   d. Pour activer la réponse partielle par lots, sélectionnez ReportBatchItemFailures.

5. Choisissez Ajouter ou Enregistrer.

Configuration du comportement en cas de nouvelle tentative (AWS CLI)

Utilisez les AWS CLI commandes suivantes pour configurer le comportement des nouvelles tentatives pour vos mappages de sources d'événements Kafka.

Création d'un mappage de sources d'événements avec des configurations de nouvelle tentative

L'exemple suivant crée un mappage de source d'événements Kafka autogéré avec des contrôles de gestion des erreurs :

```
aws lambda create-event-source-mapping \
  --function-name my-kafka-function \
  --topics my-kafka-topic \
  --source-access-configuration Type=SASL_SCRAM_512_AUTH,URI=arn:aws:secretsmanager:us-
east-1:111122223333:secret:MyBrokerSecretName \
  --self-managed-event-source '{"Endpoints":{"KAFKA_BOOTSTRAP_SERVERS":
["abc.xyz.com:9092"]}}' \
  --starting-position LATEST \
  --provisioned-poller-config MinimumPollers=1,MaximumPollers=1 \
  --maximum-retry-attempts 3 \
  --maximum-record-age-in-seconds 3600 \
  --bisect-batch-on-function-error \
  --function-response-types "ReportBatchItemFailures"
```

Pour les sources d'événements Amazon MSK :

```
aws lambda create-event-source-mapping \
  --event-source-arn arn:aws:kafka:us-east-1:111122223333:cluster/my-cluster/fc2f5bdf-
fd1b-45ad-85dd-15b4a5a6247e-2 \
  --topics AWSMSKKafkaTopic \
  --starting-position LATEST \
  --function-name my-kafka-function \
  --source-access-configurations '[{"Type": "SASL_SCRAM_512_AUTH","URI":
 "arn:aws:secretsmanager:us-east-1:111122223333:secret:my-secret"}]' \
  --provisioned-poller-config MinimumPollers=1,MaximumPollers=1 \
  --maximum-retry-attempts 3 \
  --maximum-record-age-in-seconds 3600 \
  --bisect-batch-on-function-error \
  --function-response-types "ReportBatchItemFailures"
```

Mise à jour des configurations de nouvelle tentative

Utilisez la `update-event-source-mapping` commande pour modifier les configurations de nouvelle tentative pour un mappage de source d'événement existant :

```
aws lambda update-event-source-mapping \
  --uuid 12345678-1234-1234-1234-123456789012 \
  --maximum-retry-attempts 5 \
  --maximum-record-age-in-seconds 7200 \
  --bisect-batch-on-function-error \
  --function-response-types "ReportBatchItemFailures"
```

PartialBatchResponse

La réponse partielle par lots, également connue sous le nom de ReportBatchItemFailures, est une fonctionnalité clé pour la gestion des erreurs dans l'intégration de Lambda aux sources Kafka. Sans cette fonctionnalité, lorsqu'une erreur survient dans l'un des éléments d'un lot, cela entraîne le retraitement de tous les messages de ce lot. Lorsque la réponse par lots partielle est activée et implémentée, le gestionnaire renvoie des identifiants uniquement pour les messages ayant échoué, ce qui permet à Lambda de réessayer uniquement ces éléments spécifiques. Cela permet de mieux contrôler le traitement des lots contenant des messages d'échec.

Pour signaler des erreurs par lots, utilisez ce schéma JSON :

```
{
```

```
  "batchItemFailures": [
    {
      "itemIdentifier": {
        "partition": "topic-partition_number",
        "offset": 100
      }
    },
    ...
  ]
}
```

> **Important**
>
> Si vous renvoyez un fichier JSON valide vide ou nul, le mappage de la source d'événements considère qu'un lot a été traité avec succès. Tout topic-partition_number ou offset non valide renvoyé qui n'était pas présent dans l'événement invoqué est considéré comme un échec et le lot entier est réessayé.

Les exemples de code suivants montrent comment implémenter une réponse par lots partielle pour les fonctions d'événements Lambda qui reçoivent des événements provenant de sources Kafka. La fonction signale les défaillances échecs d'articles par lots dans la réponse, en indiquant à Lambda de réessayer ces messages ultérieurement.

Voici une implémentation du gestionnaire Lambda en Python qui illustre cette approche :

```
import base64
from typing import Any, Dict, List

def lambda_handler(event: Dict[str, Any], context: Any) -> Dict[str, List[Dict[str,
 Dict[str, Any]]]]:
    failures: List[Dict[str, Dict[str, Any]]] = []
    records_dict = event.get("records", {})

    for topic_partition, records_list in records_dict.items():
        for record in records_list:
            topic = record.get("topic")
            partition = record.get("partition")
            offset = record.get("offset")
            value_b64 = record.get("value")
```

```
            try:
                data = base64.b64decode(value_b64).decode("utf-8")
                process_message(data)
            except Exception as exc:
                print(f"Failed to process record topic={topic} partition={partition}
 offset={offset}: {exc}")
                item_identifier: Dict[str, Any] = {
                    "partition": f"{topic}-{partition}",
                    "offset": int(offset) if offset is not None else None,
                }
                failures.append({"itemIdentifier": item_identifier})

    return {"batchItemFailures": failures}

def process_message(data: str) -> None:
    # Your business logic for a single message
    pass
```

Voici une Node.js version :

```
const { Buffer } = require("buffer");

const handler = async (event) => {
  const failures = [];

  for (let topicPartition in event.records) {
    const records = event.records[topicPartition];

    for (const record of records) {
      const topic = record.topic;
      const partition = record.partition;
      const offset = record.offset;
      const valueBase64 = record.value;
      const data = Buffer.from(valueBase64, "base64").toString("utf8");

      try {
        await processMessage(data);
      } catch (error) {
        console.error("Failed to process record", { topic, partition, offset, error });
        const itemIdentifier = {
          "partition": `${topic}-${partition}`,
          "offset": Number(offset),
        };
```

```
        failures.push({ itemIdentifier });
      }
    }
  }

  return { batchItemFailures: failures };
};

async function processMessage(payload) {
  // Your business logic for a single message
}

module.exports = { handler };
```

Voici une version de Java :

```
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;

import java.util.ArrayList;
import java.util.Base64;
import java.util.HashMap;
import java.util.List;
import java.util.Map;

public class KafkaBatchHandler implements RequestHandler<Map<String, Object>,
 Map<String, Object>> {

    @SuppressWarnings("unchecked")
    @Override
    public Map<String, Object> handleRequest(Map<String, Object> event, Context
 context) {
        List<Map<String, Object>> failures = new ArrayList<>();
        Map<String, List<Map<String, Object>>> records =
                (Map<String, List<Map<String, Object>>>) event.getOrDefault("records",
 Map.of());

        for (Map.Entry<String, List<Map<String, Object>>> entry : records.entrySet()) {
            for (Map<String, Object> record : entry.getValue()) {
                String topic = (String) record.get("topic");
                Object partition = record.get("partition");
                Object offset = record.get("offset");
                String valueBase64 = (String) record.get("value");
```

```
                try {
                    String data = new String(Base64.getDecoder().decode(valueBase64),
 "UTF-8");
                    processMessage(data);
                } catch (Exception e) {
                    System.err.printf("Failed to process record topic=%s partition=%s
 offset=%s: %s%n",
                            topic, partition, offset, e.getMessage());
                    Map<String, Object> itemIdentifier = new HashMap<>();
                    itemIdentifier.put("partition", topic + "-" + partition);
                    itemIdentifier.put("offset", offset instanceof Number ? ((Number)
 offset).longValue() : null);
                    Map<String, Object> failure = new HashMap<>();
                    failure.put("itemIdentifier", itemIdentifier);
                    failures.add(failure);
                }
            }
        }

        Map<String, Object> response = new HashMap<>();
        response.put("batchItemFailures", failures);
        return response;
    }

    private void processMessage(String data) {
        // Your business logic for a single message
    }
}
```

Capture de lots supprimés pour des sources d’événement Amazon MSK et Apache Kafka autogéré

Pour conserver les enregistrements des invocations de mappage des sources d'événements ayant échoué, ajoutez une destination au mappage des sources d'événements de votre fonction d'événement. Chaque enregistrement envoyé à la destination est un document JSON contenant les métadonnées sur l’invocation ayant échoué. Pour les destinations Amazon S3, Lambda envoie également l’intégralité de l’enregistrement d’invocation avec les métadonnées. Vous pouvez configurer n'importe quelle rubrique Amazon SNS, n'importe quelle file d'attente Amazon SQS, n'importe quel compartiment Amazon S3 ou Kafka comme destination.

Avec les destinations Amazon S3, vous pouvez utiliser la fonctionnalité Notifications d’événements Amazon S3 pour recevoir des notifications lorsque des objets sont chargés dans votre compartiment S3 de destination. Vous pouvez également configurer les notifications d'événements S3 pour appeler une autre fonction d'événement Lambda afin d'effectuer un traitement automatique des lots ayant échoué.

Votre rôle d’exécution doit disposer d’autorisations pour la destination :

- Pour une destination SQS : sqs : SendMessage
- Pour une destination SNS : SNS:Publish
- Pour une destination S3 : s3 : PutObject et s3 : ListBucket
- Pour une destination Kafka : kafka-cluster : WriteData

Vous pouvez configurer un sujet Kafka comme destination en cas d'échec pour vos mappages de sources d'événements Kafka. Lorsque Lambda ne parvient pas à traiter les enregistrements après avoir épuisé toutes les tentatives ou lorsque les enregistrements dépassent l'âge maximum, Lambda envoie les enregistrements ayant échoué à la rubrique Kafka spécifiée pour un traitement ultérieur. Reportez-vous à the section called “Destination de Kafka en cas d'échec”.

Vous devez déployer un point de terminaison de VPC pour votre service de destination en cas de panne au sein de votre VPC de cluster Kafka.

En outre, si vous avez configuré une clé KMS sur votre destination, Lambda a besoin des autorisations suivantes en fonction du type de destination :

- Si vous avez activé le chiffrement avec votre propre clé KMS pour une destination S3, kms : GenerateDataKey est obligatoire. Si la clé KMS et la destination du compartiment S3 se trouvent

dans un compte différent de celui de votre fonction d'événement Lambda et de votre rôle d'exécution, configurez la clé KMS de manière à ce que le rôle d'exécution autorise les km :. GenerateDataKey

- Si vous avez activé le chiffrement avec votre propre clé KMS pour la destination SQS, KMS:Decrypt et kms : sont obligatoires. GenerateDataKey Si la clé KMS et la destination de la file d'attente SQS se trouvent dans un compte différent de celui de votre fonction d'événement Lambda et de votre rôle d'exécution, configurez la clé KMS pour approuver le rôle d'exécution afin d'autoriser KMS:Decrypt, kms GenerateDataKey :, kms : et kms :. DescribeKey ReEncrypt
- Si vous avez activé le chiffrement avec votre propre clé KMS pour la destination SNS, KMS:Decrypt et kms : sont requis. GenerateDataKey Si la clé KMS et la destination de la rubrique SNS se trouvent dans un compte différent de celui de votre fonction d'événement Lambda et de votre rôle d'exécution, configurez la clé KMS pour approuver le rôle d'exécution afin d'autoriser KMS:Decrypt, kms GenerateDataKey :, kms : et kms :. DescribeKey ReEncrypt

Configuration des destinations en cas d’échec pour un mappage des sources d’événements Kafka

Pour configurer une destination en cas de panne à l’aide de la console, procédez comme suit :

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez une fonction.
3. Sous Function overview (Vue d’ensemble de la fonction), choisissez Add destination (Ajouter une destination).
4. Pour Source, choisissez Invocation du mappage des sources d’événements.
5. Pour le mappage des sources d’événements, choisissez une source d’événements configurée pour cette fonction.
6. Pour Condition, sélectionnez En cas d’échec. Pour les invocations de mappage des sources d’événements, il s’agit de la seule condition acceptée.
7. Pour Type de destination, choisissez le type de destination auquel Lambda envoie les enregistrements d’invocation.
8. Pour Destination, choisissez une ressource.
9. Cliquez sur Enregistrer.

Vous pouvez également configurer une destination en cas de panne à l’aide de l’ AWS CLI. Par exemple, la commande create-event-source-mapping suivante ajoute un mappage des sources d’événements avec une destination SQS en cas d’échec à `MyFunction` :

```
aws lambda create-event-source-mapping \
--function-name "MyFunction" \
--event-source-arn arn:aws:kafka:us-east-1:123456789012:cluster/
vpc-2priv-2pub/751d2973-a626-431c-9d4e-d7975eb44dd7-2 \
--destination-config '{"OnFailure": {"Destination": "arn:aws:sqs:us-
east-1:123456789012:dest-queue"}}'
```

La commande update-event-source-mapping ajoute une destination S3 en cas de panne à la source d'événements associée à l'entrée : `uuid`

```
aws lambda update-event-source-mapping \
--uuid f89f8514-cdd9-4602-9e1f-01a5b77d449b \
--destination-config '{"OnFailure": {"Destination": "arn:aws:s3:::dest-bucket"}}'
```

Pour supprimer une destination, entrez une chaîne vide comme argument du paramètre `destination-config` :

```
aws lambda update-event-source-mapping \
--uuid f89f8514-cdd9-4602-9e1f-01a5b77d449b \
--destination-config '{"OnFailure": {"Destination": ""}}'
```

Pratiques exemplaires en matière de sécurité pour les destinations Amazon S3

La suppression d'un compartiment S3 configuré comme destination sans supprimer la destination de la configuration de votre fonction peut engendrer un risque de sécurité. Si un autre utilisateur connaît le nom de votre compartiment de destination, il peut recréer le compartiment dans son Compte AWS. Les enregistrements des invocations ayant échoué seront envoyés dans son compartiment, exposant potentiellement les données de votre fonction.

> **Warning**
>
> Pour vous assurer que les enregistrements d'invocation de votre fonction d'événement ne peuvent pas être envoyés vers un compartiment S3 d'un autre Compte AWS, ajoutez une condition au rôle d'exécution de votre fonction qui limite `s3:PutObject` les autorisations aux compartiments de votre compte.

L'exemple suivant présente une politique IAM qui limite les autorisations `s3:PutObject` de votre fonction aux seuls compartiments de votre compte. Cette politique donne également à Lambda l'autorisation `s3:ListBucket` dont il a besoin pour utiliser un compartiment S3 comme destination.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3BucketResourceAccountWrite",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::*/*",
                "arn:aws:s3:::*"
            ],
            "Condition": {
                "StringEquals": {
                    "s3:ResourceAccount": "111122223333"
                }
            }
        }
    ]
}
```

Pour ajouter une politique d'autorisations au rôle d'exécution de votre fonction à l'aide du Console de gestion AWS ou AWS CLI, reportez-vous aux instructions des procédures suivantes :

Console

Pour ajouter une politique d'autorisations au rôle d'exécution d'une fonction (console)

1. Ouvrez la page Event Functions de la console Lambda.
2. Sélectionnez la fonction d'événement Lambda dont vous souhaitez modifier le rôle d'exécution.
3. Sous l'onglet Configuration, sélectionnez Autorisations.
4. Sous l'onglet Rôle d'exécution, sélectionnez le Nom du rôle de votre fonction pour ouvrir la page de console IAM du rôle.

5. Ajoutez une politique d'autorisations de au rôle en procédant comme suit :

   a. Dans le volet Politiques d'autorisations, choisissez Ajouter des autorisations, puis Créer une politique en ligne.

   b. Dans l'Éditeur de politique, sélectionnez JSON.

   c. Collez la politique que vous souhaitez ajouter dans l'éditeur (en remplacement du JSON existant), puis choisissez Suivant.

   d. Sous Détails de la politique, saisissez un Nom de la politique.

   e. Choisissez Create Policy (Créer une politique).

AWS CLI

Pour ajouter une politique d'autorisation au rôle d'exécution (CLI) d'une fonction d'événement

1. Créez un document de politique JSON avec les autorisations requises et enregistrez-le dans un répertoire local.
2. Utilisez la commande `put-role-policy` de la CLI IAM pour ajouter des autorisations au rôle d'exécution de votre fonction. Exécutez la commande suivante depuis le répertoire dans lequel vous avez enregistré votre document de politique JSON et remplacez le nom du rôle, le nom de la politique et le document de politique par vos propres valeurs.

```
aws iam put-role-policy \
--role-name my_lambda_role \
--policy-name LambdaS3DestinationPolicy \
--policy-document file://my_policy.json
```

Exemple d'enregistrement d'invocation SNS et SQS

L'exemple suivant montre ce que Lambda envoie à une rubrique SNS ou à une destination de file d'attente SQS pour une invocation de source d'événement Kafka qui a échoué. Chacune des clés sous `recordsInfo` contient à la fois le sujet et la partition Kafka, séparés par un trait d'union. Par exemple, pour la clé`"Topic-0"`, `Topic` est la rubrique Kafka, et `0` est la partition. Pour chaque sujet et chaque partition, vous pouvez utiliser les décalages et les données d'horodatage pour trouver les enregistrements d'invocation d'origine.

```
{
    "requestContext": {
```

```
        "requestId": "316aa6d0-8154-xmpl-9af7-85d5f4a6bc81",
        "functionArn": "arn:aws:lambda:us-east-1:123456789012:function:myfunction",
        "condition": "RetryAttemptsExhausted" | "MaximumPayloadSizeExceeded",
        "approximateInvokeCount": 1
    },
    "responseContext": { // null if record is MaximumPayloadSizeExceeded
        "statusCode": 200,
        "executedVersion": "$LATEST",
        "functionError": "Unhandled"
    },
    "version": "1.0",
    "timestamp": "2019-11-14T00:38:06.021Z",
    "KafkaBatchInfo": {
        "batchSize": 500,
        "eventSourceArn": "arn:aws:kafka:us-east-1:123456789012:cluster/
vpc-2priv-2pub/751d2973-a626-431c-9d4e-d7975eb44dd7-2",
        "bootstrapServers": "...",
        "payloadSize": 2039086, // In bytes
        "recordsInfo": {
            "Topic-0": {
                "firstRecordOffset":
 "49601189658422359378836298521827638475320189012309704722",
                "lastRecordOffset":
 "49601189658422359378836298522902373528957594348623495186",
                "firstRecordTimestamp": "2019-11-14T00:38:04.835Z",
                "lastRecordTimestamp": "2019-11-14T00:38:05.580Z",
            },
            "Topic-1": {
                "firstRecordOffset":
 "49601189658422359378836298521827638475320189012309704722",
                "lastRecordOffset":
 "49601189658422359378836298522902373528957594348623495186",
                "firstRecordTimestamp": "2019-11-14T00:38:04.835Z",
                "lastRecordTimestamp": "2019-11-14T00:38:05.580Z",
            }
        }
    }
}
```

Exemple d’enregistrement d’invocation de destination S3

Pour les destinations S3, Lambda envoie l’intégralité de l’enregistrement d’invocation ainsi que les métadonnées à la destination. L’exemple suivant montre que Lambda envoie vers une destination

de compartiment S3 en cas d'échec d'une invocation de source d'événement Kafka. Outre tous les champs de l'exemple précédent pour les destinations SQS et SNS, le champ `payload` contient l'enregistrement d'invocation d'origine sous forme de chaîne JSON échappée.

```
{
    "requestContext": {
        "requestId": "316aa6d0-8154-xmpl-9af7-85d5f4a6bc81",
        "functionArn": "arn:aws:lambda:us-east-1:123456789012:function:myfunction",
        "condition": "RetryAttemptsExhausted" | "MaximumPayloadSizeExceeded",
        "approximateInvokeCount": 1
    },
    "responseContext": { // null if record is MaximumPayloadSizeExceeded
        "statusCode": 200,
        "executedVersion": "$LATEST",
        "functionError": "Unhandled"
    },
    "version": "1.0",
    "timestamp": "2019-11-14T00:38:06.021Z",
    "KafkaBatchInfo": {
        "batchSize": 500,
        "eventSourceArn": "arn:aws:kafka:us-east-1:123456789012:cluster/
vpc-2priv-2pub/751d2973-a626-431c-9d4e-d7975eb44dd7-2",
        "bootstrapServers": "...",
        "payloadSize": 2039086, // In bytes
        "recordsInfo": {
            "Topic-0": {
                "firstRecordOffset":
 "49601189658422359378836298521827638475320189012309704722",
                "lastRecordOffset":
 "49601189658422359378836298522902373528957594348623495186",
                "firstRecordTimestamp": "2019-11-14T00:38:04.835Z",
                "lastRecordTimestamp": "2019-11-14T00:38:05.580Z",
            },
            "Topic-1": {
                "firstRecordOffset":
 "49601189658422359378836298521827638475320189012309704722",
                "lastRecordOffset":
 "49601189658422359378836298522902373528957594348623495186",
                "firstRecordTimestamp": "2019-11-14T00:38:04.835Z",
                "lastRecordTimestamp": "2019-11-14T00:38:05.580Z",
            }
        }
    },
```

```
    "payload": "<Whole Event>" // Only available in S3
}
```

> **Tip**
>
> Nous vous recommandons d'activer la gestion des versions S3 sur votre compartiment de destination.

Utiliser un sujet Kafka comme destination en cas d'échec

Vous pouvez configurer un sujet Kafka comme destination en cas d'échec pour vos mappages de sources d'événements Kafka. Lorsque Lambda ne parvient pas à traiter les enregistrements après avoir épuisé toutes les tentatives ou lorsque les enregistrements dépassent l'âge maximum, Lambda envoie les enregistrements ayant échoué à la rubrique Kafka spécifiée pour un traitement ultérieur. Lorsque vous configurez à la fois un nombre infini de tentatives et une destination en cas d'échec, Lambda applique automatiquement un maximum de 10 tentatives de tentative.

Comment fonctionne une destination Kafka en cas de défaillance

Lorsque vous configurez un sujet Kafka comme destination en cas d'échec, Lambda agit en tant que producteur Kafka et écrit les enregistrements ayant échoué dans le sujet de destination. Cela crée un modèle de sujet mort (DLT) au sein de votre infrastructure Kafka.

- Même exigence de cluster — Le sujet de destination doit exister dans le même cluster Kafka que vos sujets source.
- Contenu réel des enregistrements : les destinations Kafka reçoivent les enregistrements défaillants réels ainsi que les métadonnées relatives aux échecs.
- Prévention de la récursivité : Lambda empêche les boucles infinies en bloquant les configurations dans lesquelles les sujets source et destination sont identiques.

Authentification pour une destination Kafka

Une destination Kafka en cas de défaillance ne possède pas ses propres paramètres d'authentification. Le sujet de destination se trouve dans le même cluster que vos sujets source. Lambda écrit donc les enregistrements ayant échoué avec l'authentification que vous avez déjà configurée dans le `SourceAccessConfigurations` paramètre du mappage des sources d'événements.

Cela s'applique à toutes les méthodes d'authentification prises en charge par Lambda pour Kafka, y compris OAuth 2.0 (`OAUTHBEARER_AUTH`), IAM () et IAM with (`IAM_AUTH`). SASL/OAUTHBEARER `IAM_OAUTHBEARER_AUTH` Si vous vous authentifiez avec OAuth 2.0, Lambda utilise le même fournisseur d'identité et le même secret pour obtenir un jeton à produire vers le sujet de destination. Configurez l'authentification une seule fois, dans la configuration de l'accès à la source. Pour plus d'informations, consultez the section called “Authentification du cluster” pour Kafka autogéré et pour the section called “Authentification du cluster” Amazon MSK.

Assurez-vous que l'identité avec laquelle vous vous authentifiez peut écrire dans le sujet de destination, et pas seulement lire des extraits de vos sujets source. Pour l'authentification IAM, cela signifie qu'il s'`kafka-cluster:WriteData`agit du sujet de destination. Pour les autres méthodes, cela signifie l'autorisation d'écriture équivalente dans les règles d'autorisation de votre cluster.

Configuration d'une destination Kafka en cas de panne

Vous pouvez configurer un sujet Kafka comme destination en cas d'échec lors de la création ou de la mise à jour d'un mappage de source d'événements Kafka.

Configuration d'une destination Kafka (console)

Pour configurer un sujet Kafka comme destination en cas d'échec (console)

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez le nom de votre fonction.
3. Effectuez l'une des actions suivantes :
   - Pour ajouter un nouveau déclencheur Kafka, sous Vue d'ensemble des fonctions, choisissez Ajouter un déclencheur.
   - Pour modifier un déclencheur Kafka existant, choisissez-le, puis choisissez Modifier.
4. Sous Paramètres supplémentaires, comme On-failure destination, choisissez le sujet Kafka.
5. Dans le champ Nom du sujet, entrez le nom du sujet Kafka auquel vous souhaitez envoyer les enregistrements ayant échoué.
6. Choisissez Ajouter ou Enregistrer.

Configuration d'une destination Kafka (AWS CLI)

Utilisez le `kafka://` préfixe pour spécifier un sujet Kafka comme destination en cas d'échec.

Création d'un mappage des sources d'événements avec la destination Kafka

L'exemple suivant crée un mappage de source d'événement Amazon MSK avec un sujet Kafka comme destination en cas d'échec :

```
aws lambda create-event-source-mapping \
  --function-name my-kafka-function \
  --topics AWSKafkaTopic \
  --event-source-arn arn:aws:kafka:us-east-1:123456789012:cluster/my-cluster/abc123 \
  --starting-position LATEST \
```

```
  --provisioned-poller-config MinimumPollers=1,MaximumPollers=3 \
  --destination-config '{"OnFailure":{"Destination":"kafka://failed-records-topic"}}'
```

Pour Kafka autogéré, utilisez la même syntaxe :

```
aws lambda create-event-source-mapping \
  --function-name my-kafka-function \
  --topics AWSKafkaTopic \
  --self-managed-event-source '{"Endpoints":{"KAFKA_BOOTSTRAP_SERVERS":
["abc.xyz.com:9092"]}}' \
  --starting-position LATEST \
  --provisioned-poller-config MinimumPollers=1,MaximumPollers=3 \
  --destination-config '{"OnFailure":{"Destination":"kafka://failed-records-topic"}}'
```

Mettre à jour une destination Kafka

Utilisez la `update-event-source-mapping` commande pour ajouter ou modifier une destination Kafka :

```
aws lambda update-event-source-mapping \
  --uuid 12345678-1234-1234-1234-123456789012 \
  --destination-config '{"OnFailure":{"Destination":"kafka://failed-records-topic"}}'
```

Format d'enregistrement pour une destination Kafka

Lorsque Lambda envoie des enregistrements ayant échoué à un sujet Kafka, chaque message contient à la fois des métadonnées relatives à l'échec et le contenu réel de l'enregistrement.

Métadonnées relatives aux défaillances

Les métadonnées incluent des informations sur les raisons de l'échec de l'enregistrement et des détails sur le lot d'origine :

```
{
  "requestContext": {
    "requestId": "e4b46cbf-b738-xmpl-8880-a18cdf61200e",
    "functionArn": "arn:aws:lambda:us-east-1:123456789012:function:my-function:
$LATEST",
    "condition": "RetriesExhausted",
    "approximateInvokeCount": 3
  },
  "responseContext": {
```

```
    "statusCode": 200,
    "executedVersion": "$LATEST",
    "functionError": "Unhandled"
  },
  "version": "1.0",
  "timestamp": "2019-11-14T18:16:05.568Z",
  "KafkaBatchInfo": {
    "batchSize": 1,
    "eventSourceArn": "arn:aws:kafka:us-east-1:123456789012:cluster/my-cluster/abc123",
    "bootstrapServers": "b-1.mycluster.abc123.kafka.us-east-1.amazonaws.com:9098",
    "payloadSize": 1162,
    "recordInfo": {
      "offset": "4960118965842235937883629852182763847532018901230970472 2",
      "timestamp": "2019-11-14T18:16:04.835Z"
    }
  },
  "payload": {
    "bootstrapServers": "b-1.mycluster.abc123.kafka.us-east-1.amazonaws.com:9098",
    "eventSource": "aws:kafka",
    "eventSourceArn": "arn:aws:kafka:us-east-1:123456789012:cluster/my-cluster/abc123",
    "records": {
      "my-topic-0": [
        {
          "headers": [],
          "key": "dGVzdC1rZXk=",
          "offset": 100,
          "partition": 0,
          "timestamp": 1749116692330,
          "timestampType": "CREATE_TIME",
          "topic": "my-topic",
          "value": "dGVzdC12YWx1ZQ=="
        }
      ]
    }
  }
}
```

Comportement des clés de partition

Lambda utilise la même clé de partition que celle de l'enregistrement d'origine lors de la production vers le sujet de destination. Si l'enregistrement d'origine ne contenait aucune clé, Lambda utilise le partitionnement circulaire par défaut de Kafka entre toutes les partitions disponibles dans le sujet de destination.

Exigences et limitations

- Mode provisionné requis — Une destination Kafka en cas de défaillance n'est disponible que pour les mappages de sources d'événements avec le mode provisionné activé.
- Même cluster uniquement — Le sujet de destination doit exister dans le même cluster Kafka que vos sujets source.
- Autorisations de sujet : le mappage de la source de votre événement doit disposer d'autorisations d'écriture sur le sujet de destination. Exemple :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ClusterPermissions",
            "Effect": "Allow",
            "Action": [
                "kafka-cluster:Connect",
                "kafka-cluster:DescribeCluster",
                "kafka-cluster:DescribeTopic",
                "kafka-cluster:WriteData",
                "kafka-cluster:ReadData"
            ],
            "Resource": [
                "arn:aws:kafka:*:*:cluster/*"
            ]
        },
        {
            "Sid": "TopicPermissions",
            "Effect": "Allow",
            "Action": [
                "kafka-cluster:DescribeTopic",
                "kafka-cluster:WriteData",
                "kafka-cluster:ReadData"
            ],
            "Resource": [
                "arn:aws:kafka:*:*:topic/*/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "kafka:DescribeCluster",
```

```
                "kafka:GetBootstrapBrokers",
                "kafka:Produce"
            ],
            "Resource": "arn:aws:kafka:*:*:cluster/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups"
            ],
            "Resource": "*"
        }
    ]
}
```

- Aucune récursivité : le nom du sujet de destination ne peut pas être le même que celui de votre sujet source.

Journalisation du mappage des sources d'événements Kafka

Vous pouvez configurer la journalisation au niveau du système pour vos mappages de sources d'événements Kafka afin d'activer et de filtrer les journaux système auxquels les sondeurs d'événements Lambda envoient des informations. CloudWatch

Cette fonctionnalité n'est disponible que pour les mappages de sources d'événements Kafka et en mode provisionné.

Pour le mappage des sources d'événements avec la configuration de journalisation, vous pouvez également consulter les journaux du système à partir de requêtes de journal prédéfinies dans l'onglet Monitor de la page Console Lambda > Ressources supplémentaires > mappages de sources d'événements actuels.

Comment fonctionne la journalisation

Lorsque vous définissez la configuration de journalisation avec le niveau de journalisation dans le mappage de votre source d'événements, le sondeur d'événements Lambda envoie les journaux correspondants (journaux du système de mappage des sources d'événements).

Le mappage de la source d'événements réutilise la même destination de journal avec votre fonction d'événement Lambda. Assurez-vous que le rôle d'exécution de votre fonction d'événement Lambda dispose des autorisations de journalisation nécessaires.

Le mappage de la source d'événements aura son propre flux de journal, avec l'UUID du mappage de la date et de la source de l'événement comme nom du flux de journal, par exemple. `2020/01/01/12345678-1234-1234-1234-12345678901`

Pour les journaux du système de mappage des sources d'événements, vous pouvez choisir entre les niveaux de journal suivants.

Niveau de journalisation	Usage
DEBUG (le plus détaillé)	Informations détaillées sur la progression du traitement des sources d'événements
INFO	Messages concernant le fonctionnement normal du mappage de la source de votre événement

Niveau de journalisation	Usage
WARN (moindre détail)	Messages concernant les avertissements et les erreurs potentiels susceptibles d'entraîner un comportement inattendu

Lorsque vous sélectionnez un niveau de journal, Lambda Event Poller envoie des journaux à ce niveau ou à un niveau inférieur. Par exemple, si vous définissez le niveau de journal du système de mappage de la source d'événements sur INFO, Event Poller n'envoie pas de sorties de journal au niveau DEBUG.

Configuration de la journalisation

Vous pouvez définir la configuration de journalisation lors de la création ou de la mise à jour d'un mappage de source d'événements Kafka.

Configuration de la journalisation (console)

Pour configurer la journalisation (console)

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez le nom de votre fonction.
3. Effectuez l’une des actions suivantes :
   - Pour ajouter un nouveau déclencheur Kafka, sous Vue d'ensemble des fonctions, choisissez Ajouter un déclencheur.
   - Pour modifier un déclencheur Kafka existant, choisissez-le, puis choisissez Modifier.
4. Sous Configuration du sondeur d'événements, pour le mode provisionné, cochez la case Configurer. Et le paramètre Log level apparaîtrait.
5. Choisissez la liste déroulante des niveaux de journalisation et sélectionnez un niveau pour le mappage des sources d'événements.
6. Choisissez Ajouter ou Enregistrer en bas pour créer ou mettre à jour le mappage des sources d'événements.

Configuration de la journalisation (AWS CLI)

Création d'un mappage des sources d'événements avec journalisation

L'exemple suivant crée un mappage de source d'événement Amazon MSK avec une configuration de journalisation :

```
aws lambda create-event-source-mapping \
  --function-name my-kafka-function \
  --topics AWSKafkaTopic \
  --event-source-arn arn:aws:kafka:us-east-1:123456789012:cluster/my-cluster/abc123 \
  --starting-position LATEST \
  --provisioned-poller-config MinimumPollers=1,MaximumPollers=3 \
  --logging-config '{"SystemLogLevel":"DEBUG"}'
```

Pour Kafka autogéré, utilisez la même syntaxe :

```
aws lambda create-event-source-mapping \
  --function-name my-kafka-function \
  --topics AWSKafkaTopic \
  --self-managed-event-source '{"Endpoints":{"KAFKA_BOOTSTRAP_SERVERS":
["abc.xyz.com:9092"]}}' \
  --starting-position LATEST \
  --provisioned-poller-config MinimumPollers=1,MaximumPollers=3 \
  --logging-config '{"SystemLogLevel":"DEBUG"}'
```

Mettre à jour la configuration d'enregistrement

Utilisez la `update-event-source-mapping` commande pour ajouter ou modifier la configuration de journalisation :

```
aws lambda update-event-source-mapping \
  --uuid 12345678-1234-1234-1234-123456789012 \
  --logging-config '{"SystemLogLevel":"WARN"}'
```

Format d'enregistrement pour un journal du système de mappage des sources d'événements Kafka

Lorsque Lambda Event Poller envoie le journal, chaque entrée de journal contient des métadonnées générales de mappage des sources d'événements ainsi que du contenu spécifique à l'événement.

Enregistrement du journal WARN

L'enregistrement WARN contient des erreurs ou des avertissements provenant de l'analyseur d'événements, et il est émis lorsque l'événement s'est produit. Par exemple :

```
{
    "eventType": "ESM_PROCESSING_EVENT",
    "timestamp": 1546347650000,
    "resourceArn": "arn:aws:lambda:us-east-1:123456789012:event-source-
mapping:12345678-1234-1234-1234-123456789012",
    "eventSourceArn": "arn:aws:kafka:us-east-1:123456789012:cluster/tests-
cluster/87654321-4321-4321-4321-876543221-s1",
    "eventProcessorId": "12345678-1234-1234-1234-123456789012/0",
    "logLevel": "WARN",
    "error": {
        "errorMessage": "Timeout expired while fetching topic metadata",
        "errorCode": "org.apache.kafka.common.errors.TimeoutException"
    }
}
```

Enregistrement du journal INFO

L'enregistrement INFO contient les configurations des clients clients Kafka dans chaque sondeur d'événements, et il est émis lors de la création ou de la modification d'un consommateur. Par exemple :

```
{
    "eventType": "POLLER_STATUS_EVENT",
    "timestamp": 1546347660000,
    "resourceArn": "arn:aws:lambda:us-east-1:123456789012:event-source-
mapping:12345678-1234-1234-1234-123456789012",
    "eventSourceArn": "arn:aws:kafka:us-east-1:123456789012:cluster/tests-
cluster/87654321-4321-4321-4321-876543221-s1",
    "eventProcessorId": "12345678-1234-1234-1234-123456789012/0",
    "logLevel": "INFO",
    "kafkaEventSourceConnection": {
        "brokerEndpoints": "boot-abcd1234.c2.kafka-serverless.us-
east-1.amazonaws.com:9098",
        "consumerId": "12345678-1234-1234-1234-123456789012-0",
        "topics": [
            "test"
        ],
        "consumerGroupId": "12345678-1234-1234-1234-123456789012",
```

```
        "securityProtocol": "SASL_SSL",
        "saslMechanism": "AWS_MSK_IAM",
        "totalPartitionCount": 2,
        "assignedPartitionCount": 2,
        "partitionsAssignmentGeneration": 5,
        "assignedPartitions": [
            "test-0",
            "test-1"
        ],
        "networkConfig": {
            "ipAddresses": [
                "10.100.141.1"
            ],
            "subnetCidrBlock": "10.100.128.0/20",
            "securityGroups": [
                "sg-abcdefabcdefabcdef"
            ]
        }
    }
}
```

Enregistrement du journal DEBUG

Le journal DEBUG contient les informations relatives aux décalages de Kafka lors du traitement du mappage des sources d'événements, et les informations de décalage sont émises par minute. Par exemple :

```
{
    "eventType": "KAFKA_STATUS_EVENT",
    "timestamp": 1546347670000,
    "resourceArn": "arn:aws:lambda:us-east-1:123456789012:event-source-
mapping:12345678-1234-1234-1234-123456789012",
    "eventSourceArn": "arn:aws:kafka:us-east-1:123456789012:cluster/tests-
cluster/87654321-4321-4321-4321-876543221-s1",
    "eventProcessorId": "12345678-1234-1234-1234-123456789012/0",
    "logLevel": "DEBUG",
    "kafkaPartitionOffsets": {
        "partition": "test-1",
        "endOffset": 5004,
        "consumedOffset": 5003,
        "processedOffset": 5003,
        "committedOffset": 5004
    }
```

```
}
```

Résolution des erreurs de mappage des sources d’événements Kafka

Les rubriques suivantes fournissent des conseils de dépannage pour les erreurs et les problèmes que vous pouvez rencontrer en utilisant Amazon MSK ou Apache Kafka autogéré avec Lambda.

Pour obtenir de l’aide supplémentaire en matière de résolution des problèmes, consultez le Centre de connaissances AWS.

Authentification et erreurs d’autorisation

Si l'une des autorisations requises pour consommer les données du cluster Kafka est manquante, Lambda affiche l'un des messages d'erreur suivants dans le mappage des sources d'événements ci-dessous. LastProcessingResult

Messages d’erreur

- Le cluster n’a pas pu autoriser Lambda
- Échec de l’authentification SASL
- Le serveur n’a pas réussi à authentifier Lambda
- Lambda n’a pas réussi à authentifier le serveur
- Le certificat ou la clé privée fournis n’est pas valide

Le cluster n’a pas pu autoriser Lambda

Pour SASL/SCRAM ou mTLS, cette erreur indique que l'utilisateur fourni ne possède pas toutes les autorisations requises de la liste de contrôle d'accès (ACL) Kafka suivantes :

- DescribeConfigs Cluster
- Décrire un groupe
- Lire le groupe
- Décrire la rubrique
- Lire la rubrique

Lorsque vous créez des listes ACL Kafka avec les autorisations `kafka-cluster` requises, vous devez spécifier la rubrique et le groupe en tant que ressources. Le nom de la rubrique doit correspondre à la rubrique dans le mappage des sources d’événements. Le nom du groupe doit correspondre à l’UUID du mappage des sources d’événements.

Une fois que vous avez ajouté les autorisations requises au rôle d'exécution, il peut y avoir un délai de plusieurs minutes avant que les modifications ne prennent effet.

Voici un exemple de journal au niveau du système ESM après avoir activé Logging Config pour ce problème :

```
{
    "eventType": "ESM_PROCESSING_EVENT",
    "timestamp": 1734567890123,
    "resourceArn": "arn:aws:lambda:us-east-1:123456789012:event-source-
mapping:a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "eventSourceArn": "arn:aws:kafka:us-east-1:123456789012:cluster/my-kafka-
cluster/12345678-abcd-1234-efgh-EXAMPLE11111-1",
    "eventProcessorId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111/0",
    "logLevel": "WARN",
    "error": {
        "errorMessage": "Not authorized to access topics: [my-topic]",
        "errorCode": "org.apache.kafka.common.errors.TopicAuthorizationException"
    }
}
```

Échec de l'authentification SASL

Pour SASL/SCRAM ou SASL/PLAIN, cette erreur indique que les informations de connexion fournies ne sont pas valides.

Pour le contrôle d'accès IAM, le rôle d'exécution ne dispose pas des autorisations `kafka-cluster:Connect` pour le cluster. Ajoutez cette autorisation au rôle et spécifiez l'Amazon Resource Name (ARN) du cluster en tant que ressource.

Cette erreur peut se produire de façon intermittente. Le cluster rejette les connexions une fois que le nombre de connexions TCP dépasse le Quota de service. Lambda fait marche arrière et tente de nouveau jusqu'à ce qu'une connexion soit réussie. Une fois que Lambda se connecte au cluster et interroge les enregistrements, le dernier résultat de traitement passe à `OK`.

Voici un exemple de journal ESM au niveau du système après avoir activé Logging Config pour ce problème lors de l'utilisation de l'authentification IAM :

```
{
    "eventType": "ESM_PROCESSING_EVENT",
    "timestamp": 1734567890456,
```

```
    "resourceArn": "arn:aws:lambda:us-east-1:123456789012:event-source-
mapping:a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "eventSourceArn": "arn:aws:kafka:us-east-1:123456789012:cluster/my-kafka-
cluster/12345678-abcd-1234-efgh-EXAMPLE22222-1",
    "eventProcessorId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222/0",
    "logLevel": "WARN",
    "error": {
        "errorMessage": "[a1b2c3d4-5678-90ab-cdef-EXAMPLE22222]: Access denied",
        "errorCode": "org.apache.kafka.common.errors.SaslAuthenticationException"
    }
}
```

Le serveur n'a pas réussi à authentifier Lambda

Cette erreur indique que l'agent Kafka n'a pas réussi à authentifier Lambda. Cette erreur se produit dans les conditions suivantes :

- Vous n'avez pas fourni de certificat client pour l'authentification mTLS.
- Vous avez fourni un certificat client, mais les courtiers ne sont pas configurés pour utiliser l'authentification mTLS.
- Les courtiers Kafka ne font pas confiance à un certificat client.

Lambda n'a pas réussi à authentifier le serveur

Cette erreur indique que Lambda n'a pas réussi à authentifier l'agent Kafka. Cette erreur se produit dans les conditions suivantes :

- Pour Apache Kafka autogéré : les agents Kafka utilisent des certificats autosignés ou une autorité de certification privée, mais n'ont pas fourni le certificat CA racine du serveur.
- Pour Apache Kafka autogéré : le certificat CA racine du serveur ne correspond pas à l'autorité de certification racine qui a signé le certificat de l'agent.
- La validation du nom d'hôte a échoué, car le certificat du courtier ne contient pas le nom DNS ou l'adresse IP du courtier comme autre nom de sujet.

Le certificat ou la clé privée fournis n'est pas valide

Cette erreur indique que le consommateur Kafka n'a pas pu utiliser le certificat ou la clé privée fournis. Assurez-vous que le certificat et la clé utilisent le format PEM et que le chiffrement de la clé privée utilise un algorithme PBES1.

Voici un exemple de journal au niveau du système ESM après avoir activé Logging Config pour ce problème :

```
{
    "eventType": "ESM_PROCESSING_EVENT",
    "timestamp": 1734567891234,
    "resourceArn": "arn:aws:lambda:us-east-1:123456789012:event-source-
mapping:a1b2c3d4-5678-90ab-cdef-EXAMPLE44444",
    "eventSourceArn": "arn:aws:kafka:us-east-1:123456789012:cluster/my-kafka-
cluster/12345678-abcd-1234-efgh-EXAMPLE44444-1",
    "eventProcessorId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE44444/0",
    "logLevel": "WARN",
    "error": {
        "errorMessage": "Invalid PEM keystore configs",
        "errorCode": "org.apache.kafka.common.errors.InvalidConfigurationException"
    }
}
```

Erreurs de réseau et de connectivité

Des problèmes de configuration réseau peuvent empêcher Lambda de se connecter à votre cluster Kafka. Les rubriques suivantes décrivent les erreurs réseau courantes.

Messages d'erreur

- Délai de connexion dû à la configuration du groupe de sécurité
- Les points de terminaison du courtier Kafka ne peuvent pas être résolus

Délai de connexion dû à la configuration du groupe de sécurité

Si le groupe de sécurité associé à votre cluster Kafka n'autorise pas le trafic entrant en provenance de lui-même, Lambda ne peut pas se connecter au cluster. Assurez-vous que les règles entrantes du groupe de sécurité autorisent le trafic provenant du groupe de sécurité lui-même sur les ports du courtier Kafka.

Voici un exemple de journal au niveau du système ESM après avoir activé Logging Config pour ce problème :

```
{
    "eventType": "ESM_PROCESSING_EVENT",
    "timestamp": 1734567892345,
```

```
    "resourceArn": "arn:aws:lambda:us-east-1:123456789012:event-source-
mapping:a1b2c3d4-5678-90ab-cdef-EXAMPLE55555",
    "eventSourceArn": "arn:aws:kafka:us-east-1:123456789012:cluster/my-kafka-
cluster/12345678-abcd-1234-efgh-EXAMPLE55555-1",
    "eventProcessorId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE55555/0",
    "logLevel": "WARN",
    "error": {
        "errorMessage": "Timeout expired while fetching topic metadata",
        "errorCode": "org.apache.kafka.common.errors.TimeoutException"
    }
}
```

Vous pouvez également consulter le journal Kafka Consumer INFO pour vérifier la connexion et la configuration du réseau. Le `brokerEndpoints` champ indique les adresses du courtier Kafka `securityProtocol` et `saslMechanism` (le cas échéant) indique la méthode d'authentification, et le `networkConfig` champ indique les adresses IP, le bloc CIDR du sous-réseau et les groupes de sécurité utilisés par le mappage des sources d'événements. Vérifiez que les groupes de sécurité répertoriés autorisent le trafic entrant requis :

```
{
    "eventType": "POLLER_STATUS_EVENT",
    "timestamp": 1734567892456,
    "resourceArn": "arn:aws:lambda:us-east-1:123456789012:event-source-
mapping:a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
    "eventSourceArn": "arn:aws:kafka:us-east-1:123456789012:cluster/my-kafka-cluster/
a1b2c3d4-5678-90ab-cdef-11111EXAMPLE-1",
    "eventProcessorId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE/0",
    "logLevel": "INFO",
    "kafkaEventSourceConnection": {
        "brokerEndpoints": "boot-abcd1234.c2.kafka-serverless.us-
east-1.amazonaws.com:9098",
        "consumerId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE-0",
        "topics": [
            "my-topic"
        ],
        "consumerGroupId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
        "securityProtocol": "SASL_SSL",
        "saslMechanism": "AWS_MSK_IAM",
        "totalPartitionCount": 2,
        "assignedPartitionCount": 2,
        "partitionsAssignmentGeneration": 1,
        "assignedPartitions": [
```

```
            "my-topic-0",
            "my-topic-1"
        ],
        "networkConfig": {
            "ipAddresses": [
                "10.0.0.37"
            ],
            "subnetCidrBlock": "10.0.0.32/28",
            "securityGroups": [
                "sg-0123456789abcdef0"
            ]
        }
    }
}
```

Les points de terminaison du courtier Kafka ne peuvent pas être résolus

Cette erreur indique que le cluster Kafka n'existe pas ou a été supprimé. Vérifiez que le cluster spécifié dans le mappage des sources d'événements existe et est dans un état actif.

Voici un exemple de journal au niveau du système ESM après avoir activé Logging Config pour ce problème :

```
{
    "eventType": "ESM_PROCESSING_EVENT",
    "timestamp": 1734567893456,
    "resourceArn": "arn:aws:lambda:us-east-1:123456789012:event-source-
mapping:a1b2c3d4-5678-90ab-cdef-EXAMPLE66666",
    "eventSourceArn": "arn:aws:kafka:us-east-1:123456789012:cluster/my-kafka-
cluster/12345678-abcd-1234-efgh-EXAMPLE66666-1",
    "eventProcessorId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE66666/0",
    "logLevel": "WARN",
    "error": {
        "errorMessage": "No resolvable bootstrap urls given in bootstrap.servers",
        "errorCode": "org.apache.kafka.common.config.ConfigException"
    }
}
```

API de mappage des sources d’événements

Lorsque vous ajoutez votre cluster Apache Kafka comme source d'événements pour votre fonction d'événement Lambda, si votre fonction rencontre une erreur, votre client Kafka arrête le traitement

des enregistrements. Les consommateurs d'une partition de rubrique sont ceux qui s'abonnent à vos registres et qui les lisent et traitent. Vos autres consommateurs Kafka peuvent continuer à traiter les registres, à condition qu'ils ne rencontrent pas la même erreur.

Afin d'identifier les raisons pour lesquelles un consommateur cesse son traitement, vérifiez le champ `StateTransitionReason` dans la réponse de `EventSourceMapping`. La liste suivante décrit les erreurs de source d'événement que vous pouvez recevoir :

`ESM_CONFIG_NOT_VALID`

La configuration de mappage de source d'événement n'est pas valide.

`EVENT_SOURCE_AUTHN_ERROR`

Lambda n'a pas pu authentifier la source d'événement.

`EVENT_SOURCE_AUTHZ_ERROR`

Lambda ne dispose pas des autorisations requises pour accéder à la source d'événement.

`FUNCTION_CONFIG_NOT_VALID`

La configuration de la fonction n'est pas valide.

> **Note**
>
> Si vos registres d'événement Lambda dépassent la limite de taille autorisée de 6 Mo, il se peut qu'ils ne soient pas traités.

Invocation d'une fonction d'événement Lambda à l'aide d'un point de terminaison Amazon API Gateway

Vous pouvez créer une API Web avec un point de terminaison HTTP pour votre fonction d'événement Lambda à l'aide d'Amazon API Gateway. API Gateway fournit des outils pour créer et documenter des API Web qui acheminent les requêtes HTTP vers Lambda Event Functions. Vous pouvez sécuriser l'accès à votre API avec des contrôles d'authentification et d'autorisation. Vos API peuvent servir le trafic sur Internet ou peuvent être accessibles uniquement au sein de votre VPC.

> **Tip**
>
> Lambda propose deux méthodes pour invoquer votre fonction via un point de terminaison HTTP : API Gateway et URL de fonction Lambda. Si vous ne savez pas quelle est la meilleure méthode pour votre cas d'utilisation, consultez the section called "API Gateway ou URL de fonction".

Les ressources de votre API définissent une ou plusieurs méthodes, telles que GET ou POST. Les méthodes ont une intégration qui achemine les demandes vers une fonction d'événement Lambda ou un autre type d'intégration. Vous pouvez définir chaque ressource et méthode individuellement, ou utiliser des types de ressource et de méthode spéciaux pour correspondre à toutes les demandes adaptées à un modèle. Une ressource proxy attrape tous les chemins sous une ressource. La méthode ANY attrape toutes les méthodes HTTP.

Sections

- Choix d'un type d'API
- Ajouter un point de terminaison à votre fonction d'événement Lambda
- Intégration de proxy
- Format des événements
- Format de la réponse
- Permissions
- Exemple d'application
- Le gestionnaire d'événements de Powertools pour AWS Lambda
- Didacticiel : Utiliser Lambda avec Amazon API Gateway
- Gestion des erreurs Lambda avec une API Gateway

- Sélectionnez une méthode pour appeler votre fonction d'événement Lambda à l'aide d'une requête HTTP

Choix d’un type d’API

API Gateway prend en charge trois types d'API qui invoquent des fonctions d'événement Lambda :

- API HTTP : Une API RESTful légère à faible latence.
- API REST : Une API RESTful personnalisable et riche en fonctionnalités.
- WebSocket API : API Web qui maintient des connexions persistantes avec les clients pour une communication en duplex intégral.

Les API HTTP et les API REST sont toutes deux des API RESTful qui traitent les requêtes HTTP et les réponses renvoyées. Les API HTTP sont plus récentes et construites avec l’API API Gateway version 2. Les fonctionnalités suivantes sont nouvelles pour les API HTTP :

Fonctionnalités de l’API HTTP

- Déploiements automatiques – Lorsque vous modifiez des routages ou des intégrations, les modifications se déploient automatiquement sur des étapes pour lesquelles le déploiement automatique est activé.
- Étape par défaut – Vous pouvez créer une étape par défaut (`$default`) pour servir les demandes au chemin d’accès racine de l’URL de votre API. Pour les étapes nommées, vous devez inclure le nom de l’étape au début du chemin d’accès.
- Configuration CORS – Vous pouvez configurer votre API pour ajouter des en-têtes CORS aux réponses sortantes, au lieu de les ajouter manuellement dans votre code de fonction.

Les API REST sont les API RESTful classiques prises en charge par API Gateway depuis leur lancement. Les API REST disposent actuellement d’un plus grand nombre de fonctionnalités de personnalisation, d’intégration et de gestion.

Fonctionnalités de l’API REST

- Types d’intégration – Les API REST prennent en charge les intégrations Lambda personnalisées. Avec une intégration personnalisée, vous pouvez envoyer uniquement le corps de la requête à la fonction, ou appliquer un modèle de transformation au corps de requête avant de l’envoyer à la fonction.

- Contrôle d’accès – Les API REST prennent en charge plus d’options pour l’authentification et l’autorisation.
- Surveillance et suivi : les API REST prennent en charge le AWS X-Ray suivi et des options de journalisation supplémentaires.

Pour une comparaison détaillée, consultez Choose between HTTP APIs and REST APIs dans le Guide du développeur API Gateway.

WebSocket Les API utilisent également l'API API Gateway version 2 et prennent en charge un ensemble de fonctionnalités similaires. Utilisez une WebSocket API pour les applications qui bénéficient d'une connexion permanente entre le client et l'API. WebSocket Les API fournissent une communication en duplex intégral, ce qui signifie que le client et l'API peuvent envoyer des messages en continu sans attendre de réponse.

Les API HTTP prennent en charge un format d’événement simplifié (version 2.0). Pour un exemple d'événement provenant d'une API HTTP, voir Créer des intégrations de AWS Lambda proxy pour les API HTTP dans API Gateway.

Pour plus d'informations, voir Création d'intégrations de AWS Lambda proxy pour les API HTTP dans API Gateway.

Ajouter un point de terminaison à votre fonction d'événement Lambda

Pour ajouter un point de terminaison public à votre fonction d'événement Lambda

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez une fonction.
3. Sous Function overview (Vue d’ensemble de la fonction), choisissez Add trigger (Ajouter un déclencheur).
4. Sélectionnez API Gateway.
5. Choisissez Créer une API ou Utiliser une API existante.
    a. Nouvelle API : pour Type d’API, choisissez API HTTP. Pour plus d’informations, consultez Choix d’un type d’API.
    b. API existante : Sélectionnez l’API dans la liste déroulante ou entrez l’ID de l’API (par exemple, r3pmxmplak).
6. Pour Sécurité, choisissez Ouvrir.

7. Choisissez Ajouter.

Intégration de proxy

Les API Gateway comprennent des étapes, des ressources, des méthodes et des intégrations. L'étape et la ressource déterminent le chemin du point de terminaison :

Format du chemin d'accès de l'API

- `/prod/` – Etape `prod` et ressource racine.
- `/prod/user` – Etape `prod` et ressource `user`.
- `/dev/{proxy+}` – Routage quelconque à l'étape `dev`.
- `/` – (API HTTP) Etape par défaut et ressource racine.

Une intégration Lambda associe un chemin et une combinaison de méthodes HTTP à une fonction d'événement Lambda. Vous pouvez configurer API Gateway pour transmettre le corps de la demande HTTP tel quel (intégration personnalisée) ou pour encapsuler le corps de requête dans un document qui inclut toutes les informations de la demande, y compris les en-têtes, la ressource, le chemin et la méthode.

Pour plus d'informations, consultez Lambda proxy integrations in API Gateway.

Format des événements

Amazon API Gateway appelle votre fonction de manière synchrone avec un événement contenant une représentation JSON de la requête HTTP. Pour une intégration personnalisée, l'événement est le corps de la requête. Pour une intégration par proxy, l'événement a une structure définie. Pour obtenir un exemple d'événement de proxy à partir d'une API REST API Gateway, consultez la rubrique Input format of a Lambda function for proxy integration du guide du développeur API Gateway.

Format de la réponse

API Gateway attend une réponse de votre fonction et relaie le résultat à l'appelant. Pour une intégration personnalisée, vous définissez une réponse d'intégration et une réponse de méthode pour convertir la sortie de la fonction en réponse HTTP. Pour une intégration par proxy, la fonction doit répondre avec une représentation de la réponse dans un format spécifique.

L'exemple suivant montre un objet de réponse issu d'une Node.js fonction. L'objet de réponse représente une réponse HTTP réussie qui contient un document JSON.

Example index.mjs — Objet de réponse à l'intégration du proxy () Node.js

```
var response = {
      "statusCode": 200,
      "headers": {
        "Content-Type": "application/json"
      },
      "isBase64Encoded": false,
      "multiValueHeaders": {
        "X-Custom-Header": ["My value", "My other value"],
      },
      "body": "{\n  \"TotalCodeSize\": 104330022,\n  \"FunctionCount\": 26\n}"
    }
```

L'environnement d'exécution Lambda sérialise l'objet réponse dans JSON et l'envoie à l'API. L'API analyse la réponse et l'utilise pour créer une réponse HTTP, qu'elle envoie ensuite au client qui a fait la demande d'origine.

Example Réponse HTTP

```
< HTTP/1.1 200 OK
  < Content-Type: application/json
  < Content-Length: 55
  < Connection: keep-alive
  < x-amzn-RequestId: 32998fea-xmpl-4268-8c72-16138d629356
  < X-Custom-Header: My value
  < X-Custom-Header: My other value
  < X-Amzn-Trace-Id: Root=1-5e6aa925-ccecxmplbae116148e52f036
  <
  {
    "TotalCodeSize": 104330022,
    "FunctionCount": 26
  }
```

Permissions

Amazon API Gateway obtient l'autorisation d'appeler votre fonction à partir de la politique basée sur une ressource de la fonction. Vous pouvez accorder l'autorisation d'appel à toute une API ou accorder un accès limité à une étape, à une ressource ou à une méthode.

Lorsque vous ajoutez une API à votre fonction à l'aide de la console Lambda, de la console API Gateway ou d'un modèle AWS SAM , la politique basée sur une ressource de la fonction est mise à jour automatiquement. Voici un exemple de politique de fonction.

Example stratégie de fonction

JSON

```
{
  "Version":"2012-10-17",
  "Id": "default",
  "Statement": [
    {
      "Sid": "nodejs-apig-functiongetEndpointPermissionProd-BWDBXMPLXE2F",
      "Effect": "Allow",
      "Principal": {
        "Service": "apigateway.amazonaws.com"
      },
      "Action": "lambda:InvokeFunction",
      "Resource": "arn:aws:lambda:us-east-2:111122223333:function:nodejs-apig-
function-1G3MXMPLXVXYI",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:execute-api:us-
east-2:111122223333:ktyvxmpls1/*/GET/"
        }
      }
    }
  ]
}
```

Vous pouvez gérer manuellement les autorisations de politique de fonction à l'aide des opérations d'API suivantes :

- AddPermission
- RemovePermission
- GetPolicy

Pour accorder l'autorisation d'invocation à une API existante, utilisez la commande `add-permission`. Exemple :

```
aws lambda add-permission \
  --function-name my-function \
  --statement-id apigateway-get --action lambda:InvokeFunction \
  --principal apigateway.amazonaws.com \
  --source-arn "arn:aws:execute-api:us-east-2:123456789012:mnh1xmpli7/default/GET/"
```

Vous devriez voir la sortie suivante :

```
{
    "Statement": "{\"Sid\":\"apigateway-test-2\",\"Effect\":\"Allow\",\"Principal
\":{\"Service\":\"apigateway.amazonaws.com\"},\"Action\":\"lambda:InvokeFunction
\",\"Resource\":\"arn:aws:lambda:us-east-2:123456789012:function:my-function
\",\"Condition\":{\"ArnLike\":{\"AWS:SourceArn\":\"arn:aws:execute-api:us-
east-2:123456789012:mnh1xmpli7/default/GET\"}}}"
}
```

> **Note**
>
> Si votre fonction et votre API sont différentes Régions AWS, l'identifiant de région dans l'ARN source doit correspondre à la région de la fonction, et non à la région de l'API. Quand API Gateway appelle une fonction, elle utilise un ARN de ressource basé sur l'ARN de l'API, mais modifié pour correspondre à la Région de la fonction.

L'ARN source dans cet exemple accorde l'autorisation à une intégration sur la méthode GET de la ressource racine au cours de l'étape par défaut d'une API, avec l'ID `mnh1xmpli7`. Vous pouvez utiliser un astérisque dans l'ARN source pour accorder des autorisations à plusieurs étapes, méthodes ou ressources.

Modèles de ressources

- `mnh1xmpli7/*/GET/*` – Méthode GET sur toutes les ressources à toutes les étapes.
- `mnh1xmpli7/prod/ANY/user` – Méthode ANY sur la ressource `user` à l'étape `prod`.
- `mnh1xmpli7/*/*/*` – Toute méthode sur toutes les ressources à toutes les étapes.

Pour de plus amples informations sur l'affichage de la politique et la suppression des instructions, veuillez consulter Utilisation de politiques basées sur les ressources dans Lambda.

Exemple d'application

L'API Gateway avec Node.js exemple d'application inclut une fonction avec un AWS SAM modèle qui crée une API REST dont le AWS X-Ray suivi est activé. Il inclut également des scripts pour le déploiement, l'invocation de la fonction, le test de l'API et le nettoyage.

Le gestionnaire d'événements de Powertools pour AWS Lambda

Le gestionnaire d'événements du kit d'outils Powertools for AWS Lambda fournit le routage, le middleware, la configuration CORS, la génération de spécifications OpenAPI, la validation des demandes, la gestion des erreurs et d'autres fonctionnalités utiles lors de l'écriture de fonctions d'événement Lambda invoquées par un point de terminaison API Gateway (HTTP ou REST). L'utilitaire de gestion d'événements est disponible pour Python et TypeScript/JavaScript. Pour plus d'informations, consultez l'API REST du gestionnaire d'événements dans la documentation de Powertools pour AWS Lambda (Python) et l'API HTTP du gestionnaire d'événements dans la documentation de Powertools pour AWS Lambda (). TypeScript

Python

```
from aws_lambda_powertools import Logger
from aws_lambda_powertools.event_handler import APIGatewayRestResolver
from aws_lambda_powertools.logging import correlation_paths
from aws_lambda_powertools.utilities.typing.lambda_context import LambdaContext

app = APIGatewayRestResolver()
logger = Logger()

@app.get("/healthz")
def ping():
    return {"message": "health status ok"}

@logger.inject_lambda_context(correlation_id_path=correlation_paths.API_GATEWAY_REST)
def lambda_handler(event: dict, context: LambdaContext) -> dict:
    return app.resolve(event, context)
```

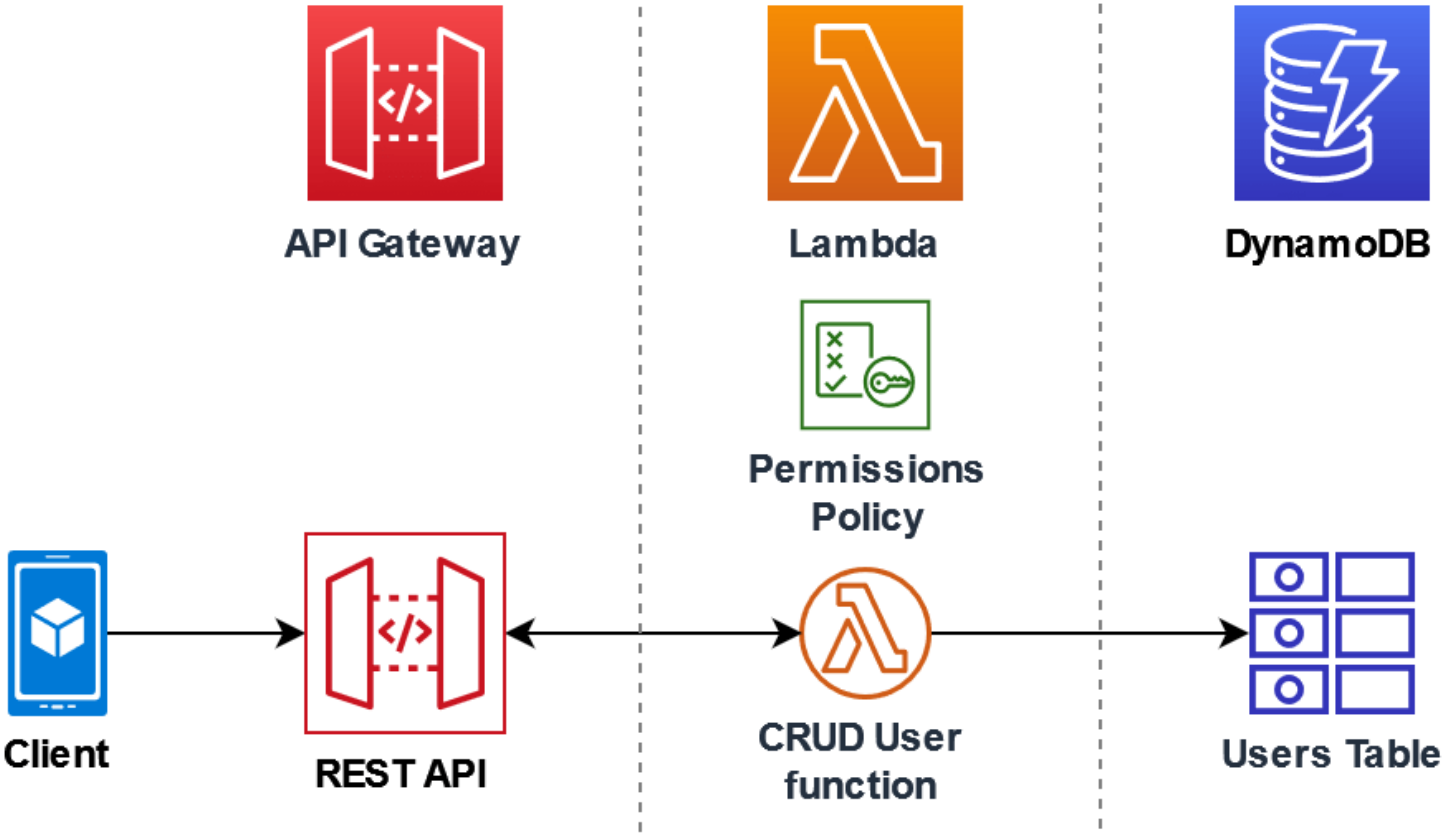
TypeScript

```
import { Router } from '@aws-lambda-powertools/event-handler/experimental-rest';
```

```
import { Logger } from '@aws-lambda-powertools/logger';
import {
  correlationPaths,
  search,
} from '@aws-lambda-powertools/logger/correlationId';
import type { Context } from 'aws-lambda/handler';

const logger = new Logger({
  correlationIdSearchFn: search,
});

const app = new Router({ logger });

app.get("/healthz", async () => {
  return { message: "health status ok" };
});

export const handler = async (event: unknown, context: Context) => {
  // You can continue using other utilities just as before
  logger.addContext(context);
  logger.setCorrelationId(event, correlationPaths.API_GATEWAY_REST);
  return app.resolve(event, context);
};
```

Didacticiel : Utiliser Lambda avec Amazon API Gateway

Dans ce didacticiel, vous allez créer une API REST par le biais de laquelle vous pouvez invoquer une fonction d'événement Lambda à l'aide d'une requête HTTP. Votre fonction d'événement Lambda effectue des opérations de création, de lecture, de mise à jour et de suppression (CRUD) sur une table DynamoDB. Cette fonction est fournie ici à titre de démonstration, mais vous apprendrez à configurer une API REST API Gateway capable d'appeler n'importe quelle fonction d'événement Lambda.



L'utilisation d'API Gateway fournit aux utilisateurs un point de terminaison HTTP sécurisé pour appeler votre fonction d'événement Lambda et peut aider à gérer de gros volumes d'appels vers votre fonction en limitant le trafic et en validant et en autorisant automatiquement les appels d'API. API Gateway fournit également des contrôles de sécurité flexibles à l'aide de Gestion des identités et des accès AWS (IAM) et d'Amazon Cognito. Ceci est utile pour les cas d'utilisation où une autorisation préalable est requise pour les appels à votre application.

> **Tip**
>
> Lambda propose deux méthodes pour invoquer votre fonction via un point de terminaison HTTP : API Gateway et URL de fonction Lambda. Si vous ne savez pas quelle est la meilleure méthode pour votre cas d'utilisation, consultez the section called "API Gateway ou URL de fonction".

Pour terminer ce didacticiel, vous devez suivre les étapes suivantes :

1. Créez et configurez une fonction d'événement Lambda en Python ou Node.js pour effectuer des opérations sur une table DynamoDB.

2. Créez une API REST dans API Gateway pour vous connecter à votre fonction d'événement Lambda.
3. Créez une table DynamoDB et testez-la avec votre fonction d'événement Lambda dans la console.
4. Déployer votre API et tester la configuration complète en utilisant curl dans un terminal.

En effectuant ces étapes, vous apprendrez à utiliser API Gateway pour créer un point de terminaison HTTP capable d'invoquer en toute sécurité une fonction d'événement Lambda à n'importe quelle échelle. Vous apprendrez également à déployer votre API, à la tester dans la console et en envoyant une requête HTTP à l'aide d'un terminal.

Création d’une stratégie d’autorisations

Avant de créer un rôle d'exécution pour votre fonction d'événement Lambda, vous devez d'abord créer une politique d'autorisation pour autoriser votre fonction à accéder aux ressources requises AWS . Pour ce didacticiel, la politique permet à Lambda d'effectuer des opérations CRUD sur une table DynamoDB et d'écrire sur Amazon Logs. CloudWatch

Pour créer la politique

1. Ouvrez la page stratégies de la console IAM.
2. Choisissez Créer une stratégie.
3. Choisissez l’onglet JSON, puis collez la stratégie personnalisée suivante dans l’éditeur JSON.

   JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1428341300017",
      "Action": [
        "dynamodb:DeleteItem",
        "dynamodb:GetItem",
        "dynamodb:PutItem",
        "dynamodb:Query",
        "dynamodb:Scan",
        "dynamodb:UpdateItem"
      ],
      "Effect": "Allow",
```

```
      "Resource": "*"
    },
    {
      "Sid": "",
      "Resource": "*",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Effect": "Allow"
    }
  ]
}
```

4. Choisissez Suivant : Balises.
5. Choisissez Suivant : Vérification.
6. Sous Examiner une stratégie, pour le Nom de la stratégie, saisissez **`lambda-apigateway-policy`**.
7. Choisissez Créer une stratégie.

Créer un rôle d’exécution

Un rôle d'exécution est un rôle Gestion des identités et des accès AWS (IAM) qui accorde à une fonction d'événement Lambda l'autorisation d' Services AWS accès et de ressources. Pour permettre à votre fonction d’effectuer des opérations sur une table DynamoDB, vous attachez la politique d’autorisation que vous avez créée à l’étape précédente.

Pour créer un rôle d’exécution et attacher votre politique d’autorisations personnalisée

1. Ouvrez la page Rôles de la console IAM.
2. Sélectionnez Créer un rôle.
3. Pour le type d’entité de confiance, choisissez Service AWS , puis pour le cas d’utilisation, choisissez Lambda.
4. Choisissez Suivant.
5. Dans la zone de recherche de stratégie, entrez **`lambda-apigateway-policy`**.
6. Dans les résultats de la recherche, sélectionnez la stratégie que vous avez créée (`lambda-apigateway-policy`), puis choisissez Suivant.

7. Sous Role details (Détails du rôle), pour Role name (Nom du rôle), saisissez **`lambda-apigateway-role`**, puis sélectionnez Create role (Créer un rôle).

Création de la fonction d'événement Lambda

1. Ouvrez la page Event Functions de la console Lambda et choisissez Create Event Function.
2. Choisissez Créer à partir de zéro.
3. Sous Nom de la fonction, saisissez `LambdaFunctionOverHttps`.
4. Pour Runtime, choisissez le dernier runtime Node.js ou Python Runtime.
5. Sous Permissions (Autorisations), développez Change default execution role (Modifier le rôle d'exécution par défaut).
6. Sélectionnez Utiliser un rôle existant, sélectionnez le rôle **`lambda-apigateway-role`** que vous avez créé précédemment.
7. Choisissez Create Event Function.
8. Dans le volet Source du code, remplacez le code par défaut par le code suivant Node.js ou le code Python.

   Node.js

   Le `region` paramètre doit correspondre à l' Région AWS endroit où vous déployez la fonction et créez la table DynamoDB.

   Example index.mjs

```
import { DynamoDBDocumentClient, PutCommand, GetCommand,
         UpdateCommand, DeleteCommand} from "@aws-sdk/lib-dynamodb";
import { DynamoDBClient } from "@aws-sdk/client-dynamodb";

const ddbClient = new DynamoDBClient({ region: "us-east-2" });
const ddbDocClient = DynamoDBDocumentClient.from(ddbClient);

// Define the name of the DDB table to perform the CRUD operations on
const tablename = "lambda-apigateway";

/**
 * Provide an event that contains the following keys:
 *
 *   - operation: one of 'create,' 'read,' 'update,' 'delete,' or 'echo'
 *   - payload: a JSON object containing the parameters for the table item
```

```
 *     to perform the operation on
 */
export const handler = async (event, context) => {

     const operation = event.operation;

     if (operation == 'echo'){
          return(event.payload);
     }

    else {
        event.payload.TableName = tablename;
        let response;

        switch (operation) {
          case 'create':
               response = await ddbDocClient.send(new
 PutCommand(event.payload));
               break;
          case 'read':
               response = await ddbDocClient.send(new
 GetCommand(event.payload));
               break;
          case 'update':
               response = ddbDocClient.send(new UpdateCommand(event.payload));
               break;
          case 'delete':
               response = ddbDocClient.send(new DeleteCommand(event.payload));
               break;
          default:
            response = 'Unknown operation: ${operation}';
          }
        console.log(response);
        return response;
    }
};
```

Python

Example lambda_function.py

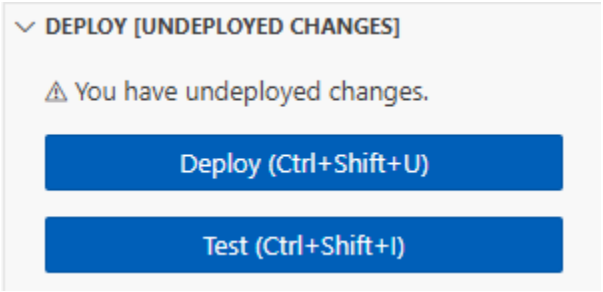
```
import boto3
```

```
# Define the DynamoDB table that Lambda will connect to
table_name = "lambda-apigateway"

# Create the DynamoDB resource
dynamo = boto3.resource('dynamodb').Table(table_name)

# Define some functions to perform the CRUD operations
def create(payload):
    return dynamo.put_item(Item=payload['Item'])

def read(payload):
    return dynamo.get_item(Key=payload['Key'])

def update(payload):
    return dynamo.update_item(**{k: payload[k] for k in ['Key',
 'UpdateExpression',
    'ExpressionAttributeNames', 'ExpressionAttributeValues'] if k in payload})

def delete(payload):
    return dynamo.delete_item(Key=payload['Key'])

def echo(payload):
    return payload

operations = {
    'create': create,
    'read': read,
    'update': update,
    'delete': delete,
    'echo': echo,
}

def lambda_handler(event, context):
    '''Provide an event that contains the following keys:
      - operation: one of the operations in the operations dict below
      - payload: a JSON object containing parameters to pass to the
        operation being performed
    '''

    operation = event['operation']
    payload = event['payload']

    if operation in operations:
        return operations[operation](payload)
```

```
    else:
        raise ValueError(f'Unrecognized operation "{operation}"')
```

> **Note**
>
> Dans cet exemple, le nom de la table DynamoDB est défini comme une variable dans le code de votre fonction. Dans une application réelle, passer ce paramètre comme une variable d'environnement et éviter de coder en dur le nom de la table constitue une bonne pratique. Pour plus d'informations, consultez la section Utilisation de variables d' AWS Lambda environnement.

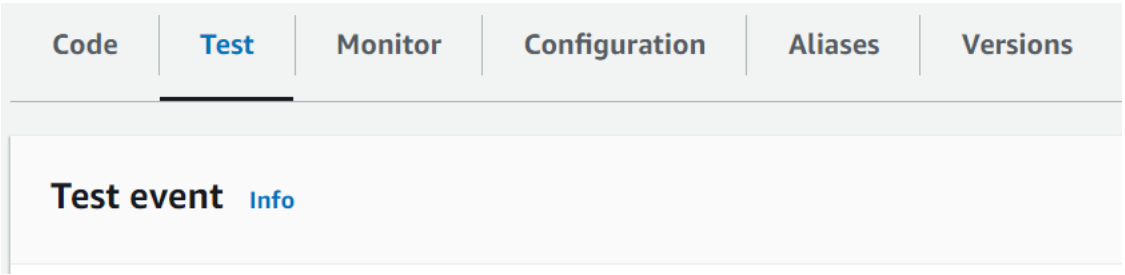
9. Dans la section DÉPLOYER, choisissez Déployer pour mettre à jour le code de votre fonction :



Tester la fonction d'événement

Avant d'intégrer votre fonction à API Gateway, confirmez que vous avez déployé la fonction avec succès. Utilisez la console Lambda pour envoyer un événement de test à votre fonction.

1. Dans la page de votre fonction de la console Lambda, choisissez l'onglet Tester.



2. Défilez jusqu'à la section JSON d'événement et remplacez l'événement par défaut par ce qui suit. Cet événement correspond à la structure attendue par la fonction d'événement Lambda.

```
{
```

```
    "operation": "echo",
    "payload": {
        "somekey1": "somevalue1",
        "somekey2": "somevalue2"
    }
}
```

3. Sélectionnez Tester).
4. Sous Exécution de la fonction : succès, développez Détails. Vous devriez voir la réponse suivante :

```
{
  "somekey1": "somevalue1",
  "somekey2": "somevalue2"
}
```

Créer une API REST avec API Gateway

Au cours de cette étape, vous créez l'API REST API Gateway que vous utilisez pour appeler votre fonction d'événement Lambda.

Pour créer l’API

1. Ouvrez la console API Gateway.
2. Sélectionnez Create API (Créer une API).
3. Dans la boîte de dialogue API REST, choisissez Créer.
4. Sous Détails de l’API, laissez Nouvelle API sélectionnée et pour Nom de l’API, saisissez **`DynamoDBOperations`**.
5. Sélectionnez Create API (Créer une API).

Créez une ressource sur votre API REST

Pour ajouter une méthode HTTP à votre API, vous devez d’abord créer une ressource pour que cette méthode puisse fonctionner. Ici, vous créez la ressource pour gérer votre table DynamoDB.

Pour créer la ressource

1. Dans la console API Gateway, sur la page Ressources de votre API, choisissez Créer une ressource.

2. Dans Détails de la ressource, pour Nom de la ressource saisissez **`DynamoDBManager`**.
3. Choisissez Create Resource.

Création d'une méthode HTTP POST

Dans cette étape, vous créez une méthode (`POST`) pour votre ressource `DynamoDBManager`. Vous liez cette `POST` méthode à votre fonction d'événement Lambda afin que, lorsque la méthode reçoit une requête HTTP, API Gateway invoque votre fonction d'événement Lambda.

> **Note**
>
> Dans le cadre de ce didacticiel, une méthode HTTP (`POST`) est utilisée pour appeler une seule fonction d'événement Lambda qui exécute toutes les opérations sur votre table DynamoDB. Dans une application réelle, la meilleure pratique consiste à utiliser une fonction d'événement Lambda et une méthode HTTP différentes pour chaque opération. Pour plus d'informations, consultez Le monolithe Lambda dans Serverless Land.

Pour créer la méthode POST

1. Sur la page Ressources de votre API, assurez-vous que la ressource `/DynamoDBManager` est surlignée. Ensuite, dans le volet Méthodes, choisissez Créer une méthode.
2. Pour Type de méthode, sélectionnez POST.
3. Pour Type d'intégration, laissez la Fonction Lambda sélectionnée.
4. Pour la Fonction Lambda, choisissez l'Amazon Resource Name (ARN) pour votre fonction (`LambdaFunctionOverHttps`).
5. Choisissez Créer une méthode.

Créez une table DynamoDB

Créez une table DynamoDB vide sur laquelle votre fonction d'événement Lambda effectue des opérations CRUD.

Créer le tableau DynamoDB

1. Ouvrez la page Tables (Tables) de la console DynamoDB.
2. Choisissez Créer un tableau.

3. Sous Détails du tableau, procédez comme suit :

    1. Sous Nom du tableau, saisissez **`lambda-apigateway`**.
    2. Pour Clé de partition, saisissez **`id`**, et conservez le type de données défini comme Chaîne.
4. Sous Table settings (Paramètres de la table), conservez les Default settings (Paramètres par défaut).
5. Choisissez Créer un tableau.

Test de l'intégration d'API Gateway, Lambda et DynamoDB

Vous êtes maintenant prêt à tester l'intégration de votre méthode API API Gateway à votre fonction d'événement Lambda et à votre table DynamoDB. À l'aide de la console API Gateway, vous envoyez des demandes directement à votre méthode `POST` en utilisant la fonction de test de la console. Dans cette étape, vous utilisez d'abord une opération `create` pour ajouter un nouvel élément à votre table DynamoDB, puis vous utilisez une opération `update` pour modifier l'élément.

Test 1 : Pour créer un nouvel élément dans votre table DynamoDB

1. Dans la console API Gateway, choisissez votre API (`DynamoDBOperations`).
2. Choisissez la méthode POST sous la ressource `DynamoDBManager`.
3. Choisissez l'onglet Test. Vous devrez peut-être choisir la flèche droite pour afficher l'onglet.
4. Sous Méthode de test, laissez les Chaînes de requête et les En-têtes vides. Pour Corps de requête, collez l'élément JSON suivant :

```
{
  "operation": "create",
  "payload": {
    "Item": {
      "id": "1234ABCD",
      "number": 5
    }
  }
}
```

5. Sélectionnez Tester).

    Les résultats qui s'affichent à la fin du test doivent indiquer le statut `200`. Ce code d'état indique que l'opération `create` a réussi.

Pour confirmer, vérifiez que votre table DynamoDB contient maintenant le nouvel élément.

6. Ouvrez la page Tables de la console DynamoDB et choisissez la table `lambda-apigateway`.
7. Choisissez Explore table items (Explorer les éléments de la table). Dans le volet Items returned (Éléments retournés), vous devriez voir un élément avec l'id `1234ABCD` et le numéro `5`. Exemple :

Test 2 : Pour mettre à jour l'élément dans votre table DynamoDB

1. Dans la Console API Gateway, revenez à l'onglet Test votre méthode POST.
2. Sous Méthode de test, laissez les Chaînes de requête et les En-têtes vides. Pour Corps de requête, collez l'élément JSON suivant :

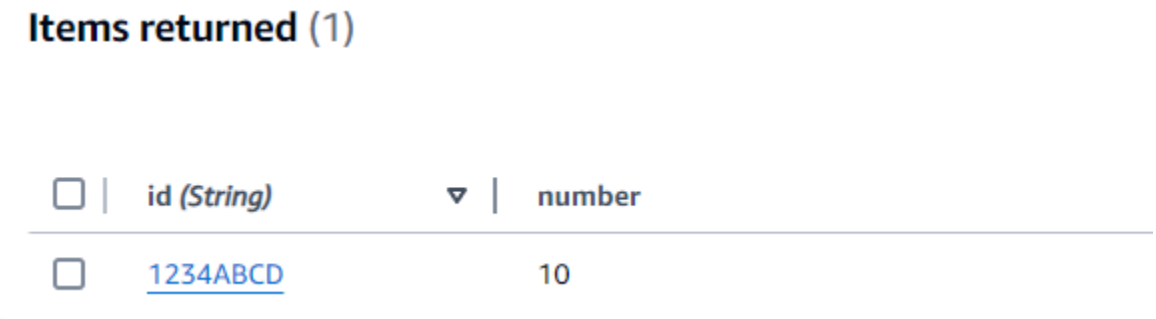
```
{
    "operation": "update",
    "payload": {
        "Key": {
            "id": "1234ABCD"
        },
        "UpdateExpression": "SET #num = :newNum",
        "ExpressionAttributeNames": {
            "#num": "number"
        },
        "ExpressionAttributeValues": {
            ":newNum": 10
        }
    }
}
```

3. Sélectionnez Tester).

Les résultats qui s'affichent à la fin du test devraient montrer l'état `200`. Ce code d'état indique que l'opération `update` a réussi.

Pour confirmer, vérifiez que l'élément dans votre table DynamoDB a été modifié.

4. Ouvrez la page Tables de la console DynamoDB et choisissez la table `lambda-apigateway`.
5. Choisissez Explore table items (Explorer les éléments de la table). Dans le volet Items returned (Éléments retournés), vous devriez voir un élément avec l'id `1234ABCD` et le numéro `10`.



Déploiement de l'API

Pour qu'un client puisse appeler l'API, vous devez créer un déploiement et une étape associée. Une étape représente un instantané de votre API, y compris ses méthodes et intégrations.

Pour déployer l'API

1. Ouvrez la page APIs (Les API) de la console API Gateway et choisissez l'API `DynamoDBOperations`.
2. Sur la page Ressources de votre API, choisissez Deploy API (Déployer l'API).
3. Pour Stage (Étape), choisissez *New stage* (Nouvelle étape), puis pour Stage name (Nom de l'étape), saisissez **`test`**.
4. Choisissez Déployer.
5. Dans le volet Stage details (Détails de l'étape), copiez Invoke URL (URL d'invocation). Vous l'utiliserez à l'étape suivante pour appeler votre fonction à l'aide d'une requête HTTP.

Utilisez curl pour appeler votre fonction d'événement à l'aide de requêtes HTTP

Vous pouvez désormais appeler votre fonction d'événement Lambda en envoyant une requête HTTP à votre API. Au cours de cette étape, vous créez un nouvel élément dans votre table DynamoDB, puis vous effectuez des opérations de lecture, de mise à jour et de suppression sur cet élément.

Pour créer un élément dans votre table DynamoDB à l'aide de curl

1. Ouvrez un terminal ou une invite de commande sur votre machine locale et exécutez la commande `curl` suivante en utilisant l'URL d'invocation que vous avez copiée à l'étape précédente. Cette commande utilise les options suivantes :

   - `-H` : ajoute un en-tête personnalisé à la demande. Ici, le paramètre spécifie le type de contenu comme étant du JSON.
   - `-d` : envoie des données dans le corps de la demande. Cette option utilise une méthode HTTP POST par défaut.

   Linux/macOS

   ```
   curl https://l8togsqxd8.execute-api.us-east-2.amazonaws.com/test/DynamoDBManager
    \
   -H "Content-Type: application/json" \
   -d '{"operation": "create", "payload": {"Item": {"id": "5678EFGH", "number":
    15}}}'
   ```

   PowerShell

   ```
   curl.exe 'https://l8togsqxd8.execute-api.us-east-2.amazonaws.com/test/
   DynamoDBManager' -H 'Content-Type: application/json' -d '{\"operation\":
    \"create\", \"payload\": {\"Item\": {\"id\": \"5678EFGH\", \"number\": 15}}}'
   ```

   Si l'opération a réussi, vous devriez voir une réponse renvoyée avec un code d'état HTTP de 200.

2. Vous pouvez également utiliser la console DynamoDB pour vérifier que le nouvel élément figure dans votre table en procédant comme suit :

   1. Ouvrez la page Tables de la console DynamoDB et choisissez la table `lambda-apigateway`.
   2. Sélectionnez Explore table items (Explorer les éléments de la table). Dans le volet Items returned (Éléments retournés), vous devriez voir un élément avec l'id `5678EFGH` et le numéro `15`.

Pour lire l'élément dans votre table DynamoDB à l'aide de curl

- Dans votre terminal ou invite de commande, exécutez la commande `curl` suivante pour lire la valeur l'élément que vous venez de créer. Utilisez votre propre URL invoquée.

  Linux/macOS

  ```
  curl https://l8togsqxd8.execute-api.us-east-2.amazonaws.com/test/DynamoDBManager
   \
  -H "Content-Type: application/json" \
  -d '{"operation": "read", "payload": {"Key": {"id": "5678EFGH"}}}'
  ```

  PowerShell

  ```
  curl.exe 'https://l8togsqxd8.execute-api.us-east-2.amazonaws.com/test/
  DynamoDBManager' -H 'Content-Type: application/json' -d '{\"operation\": \"read
  \", \"payload\": {\"Key\": {\"id\": \"5678EFGH\"}}}'
  ```

  Vous devriez obtenir un résultat semblable à l'un des suivants selon que vous avez choisi le code de fonction Node.js ou le code de fonction Python :

  Node.js

  ```
  {"$metadata":
  {"httpStatusCode":200,"requestId":"7BP3G5Q0C0O1E50FBQI9NS099JVV4KQNSO5AEMVJF66Q9ASUAAJG"
  "attempts":1,"totalRetryDelay":0},"Item":{"id":"5678EFGH","number":15}}
  ```

  Python

  ```
  {"Item":{"id":"5678EFGH","number":15},"ResponseMetadata":
  {"RequestId":"QNDJICE52E86B82VETR6RKBE5BVV4KQNSO5AEMVJF66Q9ASUAAJG",
  "HTTPStatusCode":200,"HTTPHeaders":{"server":"Server","date":"Wed, 31 Jul 2024
   00:37:01 GMT","content-type":"application/x-amz-json-1.0",
  "content-length":"52","connection":"keep-alive","x-amzn-
  requestid":"QNDJICE52E86B82VETR6RKBE5BVV4KQNSO5AEMVJF66Q9ASUAAJG","x-amz-
  crc32":"2589610852"},
  "RetryAttempts":0}}
  ```

Pour mettre à jour l'élément dans votre table DynamoDB à l'aide de curl

1. Dans votre terminal ou invite de commande, exécutez la commande `curl` suivante pour mettre à jour l'élément que vous venez de créer en modifiant la valeur `number`. Utilisez votre propre URL invoquée.

   Linux/macOS

   ```
   curl https://l8togsqxd8.execute-api.us-east-2.amazonaws.com/test/DynamoDBManager
    \
   -H "Content-Type: application/json" \
   -d '{"operation": "update", "payload": {"Key": {"id": "5678EFGH"},
    "UpdateExpression": "SET #num = :new_value", "ExpressionAttributeNames":
    {"#num": "number"}, "ExpressionAttributeValues": {":new_value": 42}}}'
   ```

   PowerShell

   ```
   curl.exe 'https://l8togsqxd8.execute-api.us-east-2.amazonaws.com/test/
   DynamoDBManager' -H 'Content-Type: application/json' -d '{\"operation\":
    \"update\", \"payload\": {\"Key\": {\"id\": \"5678EFGH\"}, \"UpdateExpression
   \": \"SET #num = :new_value\", \"ExpressionAttributeNames\": {\"#num\": \"number
   \"}, \"ExpressionAttributeValues\": {\":new_value\": 42}}}'
   ```

2. Pour confirmer que la valeur de `number` de l'élément a été mise à jour, exécutez une autre commande de lecture :

   Linux/macOS

   ```
   curl https://l8togsqxd8.execute-api.us-east-2.amazonaws.com/test/DynamoDBManager
    \
   -H "Content-Type: application/json" \
   -d '{"operation": "read", "payload": {"Key": {"id": "5678EFGH"}}}'
   ```

   PowerShell

   ```
   curl.exe 'https://l8togsqxd8.execute-api.us-east-2.amazonaws.com/test/
   DynamoDBManager' -H 'Content-Type: application/json' -d '{\"operation\": \"read
   \", \"payload\": {\"Key\": {\"id\": \"5678EFGH\"}}}'
   ```

Pour supprimer l'élément dans votre table DynamoDB à l'aide de curl

1. Dans votre terminal ou invite de commande, exécutez la commande `curl` suivante pour supprimer l'élément que vous venez de créer. Utilisez votre propre URL invoquée.

   Linux/macOS

   ```
   curl https://l8togsqxd8.execute-api.us-east-2.amazonaws.com/test/DynamoDBManager
    \
   -H "Content-Type: application/json" \
   -d '{"operation": "delete", "payload": {"Key": {"id": "5678EFGH"}}}'
   ```

   PowerShell

   ```
   curl.exe 'https://l8togsqxd8.execute-api.us-east-2.amazonaws.com/test/
   DynamoDBManager' -H 'Content-Type: application/json' -d '{\"operation\":
    \"delete\", \"payload\": {\"Key\": {\"id\": \"5678EFGH\"}}}'
   ```

2. Confirmez que l'opération de suppression a réussi. Dans le volet Items returned (Éléments retournés) de la page Explore items (Explorer les éléments) de la console DynamoDB, vérifiez que l'élément avec l'id `5678EFGH` n'est plus dans la table.

Nettoyer vos ressources (facultatif)

Vous pouvez maintenant supprimer les ressources que vous avez créées pour ce didacticiel, sauf si vous souhaitez les conserver. En supprimant AWS les ressources que vous n'utilisez plus, vous évitez des frais inutiles pour votre Compte AWS.

Pour supprimer la fonction d'événement Lambda

1. Ouvrez la page Event Functions de la console Lambda.
2. Sélectionnez la fonction d'événement que vous avez créée.
3. Sélectionnez Actions, Supprimer.
4. Saisissez **`confirm`** dans la zone de saisie de texte et choisissez Delete (Supprimer).

Pour supprimer le rôle d'exécution

1. Ouvrez la page Roles (Rôles) de la console IAM.
2. Sélectionnez le rôle d'exécution que vous avez créé.

3. Sélectionnez Supprimer.
4. Saisissez le nom du rôle dans le champ de saisie de texte et choisissez Delete (Supprimer).

Pour supprimer l'API

1. Ouvrez la page API de la console API Gateway.
2. Sélectionnez l'API que vous avez créée.
3. Sélectionnez Actions, Supprimer.
4. Sélectionnez Supprimer.

Pour supprimer la table DynamoDB

1. Ouvrez la page Tables (Tables) de la console DynamoDB.
2. Sélectionnez la table que vous avez créée.
3. Choisissez Supprimer.
4. Saisissez **`delete`** dans la zone de texte.
5. Choisissez Supprimer la table.

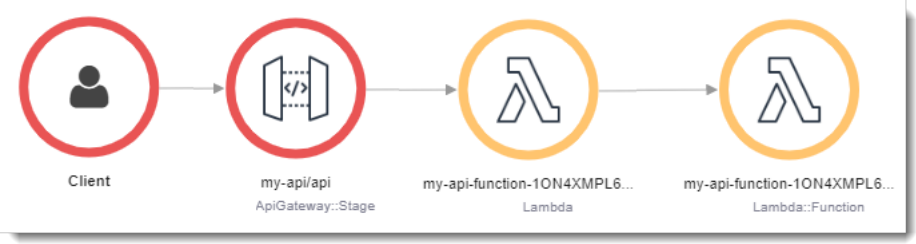
Si vous rencontrez des erreurs lors de l'appel de votre fonction via API Gateway, consultezthe section called "Erreurs".

Gestion des erreurs Lambda avec une API Gateway

API Gateway traite toutes les erreurs d'invocation et de fonction d'événement comme des erreurs internes. Si l'API Lambda rejette la demande d'invocation, API Gateway renvoie un code d'erreur 500. Si la fonction d'événement s'exécute mais renvoie une erreur ou renvoie une réponse au format incorrect, API Gateway renvoie un 502. Dans les deux cas, le corps de la réponse d'API Gateway est `{"message": "Internal server error"}`.

> **Note**
>
> API Gateway ne fait aucune nouvelle tentative d'appel Lambda. Si Lambda renvoie une erreur, API Gateway renvoie une réponse d'erreur au client.

L'exemple suivant montre une carte de X-Ray trace pour une demande qui a entraîné une erreur de fonction et un 502 provenant d'API Gateway. Le client reçoit le message d'erreur générique.

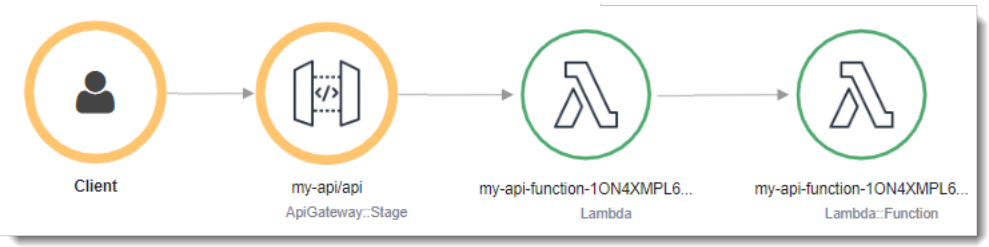


Pour personnaliser la réponse d'erreur, vous devez attraper les erreurs dans votre code et formater une réponse dans le format requis.

Example index.mjs — Erreur lors du formatage

```
var formatError = function(error){
  var response = {
    "statusCode": error.statusCode,
    "headers": {
      "Content-Type": "text/plain",
      "x-amzn-ErrorType": error.code
    },
    "isBase64Encoded": false,
    "body": error.code + ": " + error.message
  }
  return response
}
```

API Gateway convertit cette réponse en une erreur HTTP avec un code d'état et un corps personnalisés. Dans la carte de trace, le nœud de fonction est vert car il a géré l'erreur.



Sélectionnez une méthode pour appeler votre fonction d'événement Lambda à l'aide d'une requête HTTP

De nombreux cas d'utilisation courants de Lambda impliquent l'appel de votre fonction d'événement à l'aide d'une requête HTTP. Vous pourriez souhaiter qu'une application Web invoque votre fonction

par le biais d'une demande de navigateur. Les fonctions d'événement Lambda peuvent également être utilisées pour créer des API REST complètes, gérer les interactions des utilisateurs à partir d'applications mobiles, traiter des données provenant de services externes via des appels HTTP ou créer des webhooks personnalisés.

Les sections suivantes expliquent quels sont vos choix pour invoquer Lambda via HTTP et fournissent des informations qui vous aideront à prendre la bonne décision pour votre cas d'utilisation particulier.

Options proposées lors de la sélection d'une méthode d'appel HTTP

Lambda propose deux méthodes principales pour invoquer une fonction à l'aide d'une requête HTTP : les URL de fonctions et API Gateway. Les principales différences entre ces deux options sont les suivantes :

- Les URL des fonctions Lambda fournissent un point de terminaison HTTP simple et direct pour une fonction d'événement Lambda. Ils sont optimisés pour des raisons de simplicité et de rentabilité et constituent le moyen le plus rapide d'exposer une fonction d'événement Lambda via HTTP.
- API Gateway est un service plus avancé permettant de créer des API complètes. API Gateway est optimisé pour créer et gérer des API de production à grande échelle et fournit des outils complets pour la sécurité, la surveillance et la gestion du trafic.

Recommandations si vous connaissez déjà vos besoins

Si vous connaissez déjà bien vos besoins, voici nos recommandations de base :

Nous recommandons les URL de fonction pour les applications simples ou le prototypage lorsque vous n'avez besoin que de méthodes d'authentification et de request/response manipulation de base et lorsque vous souhaitez réduire les coûts et la complexité au minimum.

API Gateway est un meilleur choix pour les applications de production à grande échelle ou pour les cas où vous avez besoin de fonctionnalités plus avancées telles que la prise en charge d'OpenAPI Description, un choix d'options d'authentification, des noms de domaine personnalisés ou une request/response gestion riche, notamment la régulation, la mise en cache et la transformation. request/response

Éléments à prendre en compte lors de la sélection d'une méthode pour appeler votre fonction d'événement Lambda

Lorsque vous choisissez entre les URL de fonctions et API Gateway, vous devez prendre en compte les facteurs suivants :

- Vos besoins en matière d’authentification, par exemple si vous avez besoin d’OAuth ou d’Amazon Cognito pour authentifier les utilisateurs
- Vos exigences en matière de mise à l’échelle et la complexité de l’API que vous souhaitez implémenter
- Si vous avez besoin de fonctionnalités avancées telles que la validation et le request/response formatage des demandes
- Vos besoins en matière de surveillance
- Vos objectifs en matière de coûts

La compréhension de ces facteurs vous permettra de choisir l’option qui répond le mieux à vos exigences en matière de sécurité, de complexité et de coût.

Le tableau suivant résume les différences entre les deux options.

Authentification

- Les URL des fonctions fournissent des options d'authentification de base via Gestion des identités et des accès AWS (IAM). Vous pouvez configurer vos points de terminaison pour qu’ils soient publics (aucune authentification) ou pour qu’ils nécessitent une authentification IAM. Avec l'authentification IAM, vous pouvez utiliser des AWS informations d'identification standard ou des rôles IAM pour contrôler l'accès. Bien que simple à configurer, cette approche offre des options limitées par rapport aux autres méthodes d’authentification.
- API Gateway donne accès à une gamme plus complète d’options d’authentification. Outre l'authentification IAM, vous pouvez utiliser les autorisateurs Lambda (logique d'authentification personnalisée), les groupes d'utilisateurs et les flux Amazon Cognito. OAuth2.0 Cette flexibilité vous permet de mettre en œuvre des schémas d’authentification complexes, notamment des fournisseurs d’authentification tiers, une authentification basée sur des jetons et une authentification multifactorielle.

Request/response manipulation

- Les URL de fonctions fournissent une gestion de base des requêtes et des réponses HTTP. Elles prennent en charge les méthodes HTTP standard et créent une prise en charge intégrée du partage des ressources entre origines (CORS, cross-origin resource sharing). Bien qu'elles puissent gérer naturellement les charges utiles JSON et les paramètres de requête, elles n'offrent pas de fonctionnalités de transformation ou de validation des requêtes. La gestion des réponses est tout aussi simple : le client reçoit la réponse de votre fonction d'événement Lambda exactement telle que Lambda la renvoie.
- API Gateway fournit des fonctionnalités sophistiquées de gestion des requêtes et des réponses. Vous pouvez définir des validateurs de demandes, transformer les demandes et les réponses à l'aide de modèles de mappage, configurer request/response des en-têtes et implémenter la mise en cache des réponses. API Gateway prend également en charge les charges utiles binaires et les noms de domaine personnalisés et peut modifier les réponses avant qu'elles n'atteignent le client. Vous pouvez configurer des modèles pour la request/response validation et la transformation à l'aide du schéma JSON.

Mise à l'échelle

- Les URL des fonctions s'adaptent directement aux limites de simultanéité de votre fonction d'événement Lambda et gèrent les pics de trafic en redimensionnant votre fonction jusqu'à sa limite de simultanéité maximale configurée. Une fois cette limite atteinte, Lambda répond aux requêtes supplémentaires avec des réponses HTTP 429. Il n'existe aucun mécanisme de mise en file d'attente intégré. La gestion du dimensionnement dépend donc entièrement de la configuration de votre fonction d'événement Lambda. Par défaut, les fonctions d'événement Lambda sont limitées à 1 000 exécutions simultanées par fonction. Région AWS
- API Gateway fournit des fonctionnalités de dimensionnement supplémentaires en plus de la propre mise à l'échelle de Lambda. Il inclut des commandes intégrées de mise en file d'attente et de limitation des requêtes, ce qui vous permet de gérer les pics de trafic de manière plus élégante. API Gateway peut traiter jusqu'à 10 000 requêtes par seconde et par région par défaut, avec une capacité de débordement de 5 000 requêtes par seconde. Il fournit également des outils pour limiter les requêtes à différents niveaux (API, étape ou méthode) afin de protéger votre dorsal.

Contrôle

- Les URL des fonctions offrent une surveillance de base via CloudWatch les métriques Amazon, notamment le nombre de demandes, la latence et les taux d'erreur. Vous avez accès aux métriques et aux journaux Lambda standard, qui indiquent les requêtes brutes entrant dans votre fonction. Bien que cela fournisse une visibilité opérationnelle essentielle, les métriques se concentrent principalement sur l'exécution des fonctions.
- API Gateway fournit des fonctionnalités de surveillance complètes, notamment des métriques détaillées, des options de journalisation et de suivi. Vous pouvez surveiller les appels d'API, la latence, les taux d'erreur et hit/miss les taux de cache via CloudWatch. API Gateway s'intègre également au AWS X-Ray traçage distribué et fournit des formats de journalisation personnalisables.

Coût

- Les URL de fonctions suivent le modèle de tarification Lambda standard : vous ne payez que pour les appels de fonctions et le temps de calcul. Il n'y a pas de frais supplémentaires pour le point de terminaison de l'URL lui-même. Cela en fait un choix rentable pour les API simples ou les applications à faible trafic si vous n'avez pas besoin des fonctionnalités supplémentaires d'API Gateway.
- API Gateway propose un niveau gratuit qui inclut un million d'appels d'API reçus pour les API REST et un million d'appels d'API reçus pour les API HTTP. Ensuite, API Gateway facture les appels d'API, le transfert de données et la mise en cache (si activée). Reportez-vous à la page de tarification d'API Gateway pour connaître les coûts associés à votre propre cas d'utilisation.

Autres fonctions

- Les URL de fonctions sont conçues dans un souci de simplicité et d'intégration directe avec Lambda. Elles prennent en charge les points de terminaison HTTP et HTTPS, offrent une prise en charge CORS intégrée et créent des points de terminaison à double pile (IPv4 et IPv6). Bien qu'ils ne disposent pas de fonctionnalités avancées, ils excellent dans les scénarios où vous avez besoin d'un moyen simple et rapide d'exposer les fonctions d'événement Lambda via HTTP.
- API Gateway inclut de nombreuses fonctionnalités supplémentaires telles que le versionnement des API, la gestion des étapes, les clés d'API pour les plans d'utilisation, la documentation des API, les WebSocket API Swagger/OpenAPI, les API privées au sein d'un VPC et l'intégration WAF

pour une sécurité accrue. Il prend également en charge les déploiements Canary, les intégrations fictives à des fins de test et l'intégration avec d'autres solutions que Services AWS Lambda.

Sélectionnez une méthode pour appeler votre fonction d'événement Lambda

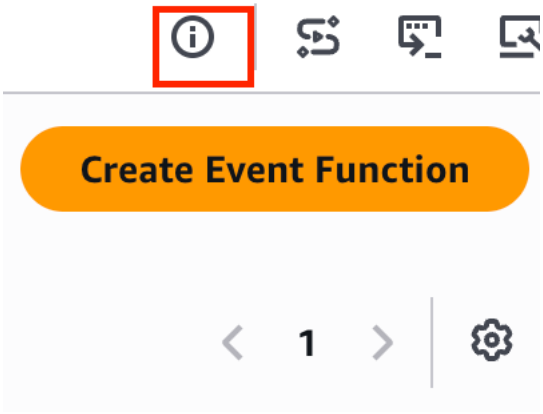
Maintenant que vous avez pris connaissance des critères de sélection entre les URL de fonctions Lambda et API Gateway et des principales différences entre les deux, vous pouvez sélectionner l'option qui répond le mieux à vos besoins et utiliser les ressources suivantes pour vous aider à commencer à l'utiliser.

Function URLs

Mise en route avec les URL de fonctions grâce aux ressources suivantes

- Suivez le didacticiel Création d'une fonction d'événement Lambda avec une URL de fonction
- Pour en savoir plus sur les URL de fonctions, consultez le chapitre the section called "URL de fonctions" de ce guide
- Essayez le tutoriel guidé intégré à la console Créer une application Web simple en procédant comme suit :

1. Ouvrez la page Event Functions de la console Lambda.
2. Ouvrez le panneau d'aide en cliquant sur l'icône dans le coin supérieur droit de l'écran.



3. Sélectionnez Tutoriels.
4. Dans Créer une application Web simple, choisissez Démarrer le tutoriel.

API Gateway

Mise en route avec Lambda et API Gateway grâce aux ressources suivantes

- Suivez le didacticiel Utilisation de Lambda avec API Gateway pour créer une API REST intégrée à une fonction d'événement Lambda principale.
- Pour en savoir plus sur les différents types d'API proposés par API Gateway, consultez les sections suivantes du Guide du développeur Amazon API Gateway :
  - API REST d'API Gateway
  - API HTTP d'API Gateway
  - API Gateway (WebSocket API)
- Essayez un ou plusieurs des exemples de la section Tutoriels et ateliers du manuel Guide du développeur Amazon API Gateway.

Utilisation AWS Lambda avec AWS Infrastructure Composer

AWS Infrastructure Composer est un constructeur visuel permettant de concevoir des applications modernes sur AWS. Vous concevez l'architecture de votre application en faisant glisser, en regroupant et Services AWS en connectant dans un canevas visuel. Infrastructure Composer crée des modèles d'infrastructure en tant que code (IaC) à partir de votre conception que vous pouvez déployer en utilisant AWS SAM ou CloudFormation.

Exportation d'une fonction d'événement Lambda vers Infrastructure Composer

Vous pouvez commencer à utiliser Infrastructure Composer en créant un nouveau projet basé sur la configuration d'une fonction d'événement Lambda existante à l'aide de la console Lambda. Pour exporter la configuration et le code de votre fonction vers Infrastructure Composer afin de créer un nouveau projet, procédez comme suit :

1. Ouvrez la page Event Functions de la console Lambda.
2. Sélectionnez la fonction que doit utiliser comme base pour votre projet Infrastructure Composer.
3. Dans le volet Présentation de la fonction, choisissez Exporter vers Infrastructure Composer.

   Pour exporter la configuration et le code de votre fonction vers Infrastructure Composer, Lambda crée un compartiment Amazon S3 dans votre compte pour stocker temporairement ces données.

4. Dans la boîte de dialogue, choisissez Confirmer et créer un projet pour accepter le nom par défaut de ce compartiment et exporter la configuration et le code de votre fonction vers Infrastructure Composer.
5. (Facultatif) Pour choisir un autre nom pour le compartiment Amazon S3 créé par Lambda, entrez un nouveau nom et choisissez Confirmer et créer un projet. Les noms de compartiment Amazon S3 doivent être uniques et respecter les règles de dénomination de compartiment.
6. Pour enregistrer vos fichiers de projet et de fonction dans Infrastructure Composer, activez le mode de synchronisation locale.

> **Note**
>
> Si vous avez déjà utilisé la fonctionnalité Exporter vers Application Composer et créé un compartiment Amazon S3 en utilisant le nom par défaut, Lambda peut réutiliser ce compartiment s'il existe toujours. Acceptez le nom du compartiment par défaut dans la boîte de dialogue pour réutiliser le compartiment existant.

Configuration des compartiments de transfert Amazon S3 Transfer AccelAccelAccel

Le compartiment Amazon S3 créé par Lambda pour transférer la configuration de votre fonction chiffre automatiquement les objets à l'aide de la norme de chiffrement AES 256. Lambda configure également le bucket pour utiliser la condition de propriétaire du bucket afin de garantir que vous Compte AWS êtes le seul à pouvoir ajouter des objets au bucket.

Lambda configure le compartiment pour qu'il supprime automatiquement les objets 10 jours après leur téléchargement. Toutefois, Lambda ne supprime pas automatiquement le compartiment lui-même. Pour supprimer le bucket de votre Compte AWS, suivez les instructions de la section Supprimer un bucket. Le nom du compartiment par défaut utilise le préfixe`lambdasam`, une chaîne alphanumérique à 10 chiffres, et Région AWS vous avez créé votre fonction dans :

```
lambdasam-06f22da95b-us-east-1
```

Pour éviter que des frais supplémentaires ne soient ajoutés à votre compte Compte AWS, nous vous recommandons de supprimer le compartiment Amazon S3 dès que vous avez terminé d'exporter votre fonction vers Infrastructure Composer.

La tarification standard d'Amazon S3 s'applique.

Autorisations requises

Pour utiliser la fonctionnalité d'intégration de Lambda à Infrastructure Composer, vous devez disposer de certaines autorisations pour télécharger un AWS SAM modèle et écrire la configuration de votre fonction sur Amazon S3.

Pour télécharger un AWS SAM modèle, vous devez être autorisé à utiliser les actions d'API suivantes :

- GetPolicy
- iam : GetPolicyVersion
- iam : GetRole
- iam : GetRolePolicy
- iam : ListAttachedRolePolicies
- iam : ListRolePolicies
- iam : ListRoles

Vous pouvez autoriser l'utilisation de toutes ces actions en ajoutant la politique Lambda_ReadOnlyAccess AWS gérée par AWS à votre rôle d'utilisateur IAM.

Pour que Lambda puisse écrire la configuration de votre fonction sur Amazon S3, vous devez être autorisé à utiliser les actions d’API suivantes :

- S3:PutObject
- S3:CreateBucket
- S3:PutBucketEncryption
- S3:PutBucketLifecycleConfiguration

Si vous ne pouvez pas exporter la configuration de votre fonction vers Infrastructure Composer, vérifiez que votre compte dispose des autorisations requises pour ces opérations. Si vous avez les autorisations requises mais que vous ne pouvez toujours pas exporter la configuration de votre fonction, vérifiez les politiques basées sur les ressources qui pourraient limiter l’accès Amazon S3.

Autres ressources

Pour un didacticiel plus détaillé sur la conception d'une application sans serveur dans Infrastructure Composer sur la base d'une fonction d'événement Lambda existante, voir. the section called “Infrastructure en tant que code (IaC)”

Pour utiliser Infrastructure Composer et concevoir et déployer une application sans serveur complète AWS SAM à l'aide de Lambda, vous pouvez également suivre AWS Infrastructure Composer le didacticiel du Serverless Patterns AWS Workshop.

Utilisation AWS Lambda avec CloudFormation

Dans un AWS CloudFormation modèle, vous pouvez spécifier une fonction d'événement Lambda comme cible d'une ressource personnalisée. Utilisez des ressources personnalisées pour traiter les paramètres, récupérer les valeurs de configuration ou appeler d'autres personnes Services AWS lors des événements du cycle de vie de la pile.

L'exemple suivant appelle une fonction qui est définie ailleurs dans le modèle.

Example– Définition de ressource personnalisée

```
Resources:
  primerinvoke:
    Type: AWS::CloudFormation::CustomResource
    Version: "1.0"
    Properties:
      ServiceToken: !GetAtt primer.Arn
      FunctionName: !Ref randomerror
```

Le jeton de service est l'Amazon Resource Name (ARN) de la fonction CloudFormation invoquée lorsque vous créez, mettez à jour ou supprimez la pile. Vous pouvez également inclure des propriétés supplémentaires telles que`FunctionName`, qui CloudFormation sont transmises telles quelles à votre fonction.

CloudFormation invoque votre fonction d'événement Lambda de manière asynchrone avec un événement qui inclut une URL de rappel.

Example– CloudFormation événement de message

```
{
    "RequestType": "Create",
    "ServiceToken": "arn:aws:lambda:us-east-1:123456789012:function:lambda-error-
processor-primer-14ROR2T3JKU66",
    "ResponseURL": "https://cloudformation-custom-resource-response-useast1.s3-us-
east-1.amazonaws.com/arn%3Aaws%3Acloudformation%3Aus-east-1%3A123456789012%3Astack/
lambda-error-processor/1134083a-2608-1e91-9897-022501a2c456%7Cprimerinvoke
%7C5d478078-13e9-baf0-464a-7ef285ecc786?
AWSAccessKeyId=AKIAIOSFODNN7EXAMPLE&Expires=1555451971&Signature=28UijZePE5I4dvukKQqM
%2F9Rf1o4%3D",
    "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/lambda-error-
processor/1134083a-2608-1e91-9897-022501a2c456",
    "RequestId": "5d478078-13e9-baf0-464a-7ef285ecc786",
```

```
    "LogicalResourceId": "primerinvoke",
    "ResourceType": "AWS::CloudFormation::CustomResource",
    "ResourceProperties": {
        "ServiceToken": "arn:aws:lambda:us-east-1:123456789012:function:lambda-error-
processor-primer-14ROR2T3JKU66",
        "FunctionName": "lambda-error-processor-randomerror-ZWUC391MQAJK"
    }
}
```

La fonction se charge de renvoyer à l'URL de rappel une réponse indiquant le succès ou l'échec. Pour obtenir la syntaxe de réponse complète, consultez Objets de réponse des ressources personnalisées.

Example– CloudFormation réponse personnalisée aux ressources

```
{
    "Status": "SUCCESS",
    "PhysicalResourceId": "2019/04/18/[$LATEST]b3d1bfc65f19ec610654e4d9b9de47a0",
    "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/lambda-error-
processor/1134083a-2608-1e91-9897-022501a2c456",
    "RequestId": "5d478078-13e9-baf0-464a-7ef285ecc786",
    "LogicalResourceId": "primerinvoke"
}
```

CloudFormation fournit une bibliothèque appelée `cfn-response` qui gère l'envoi de la réponse. Si vous définissez votre fonction dans un modèle, vous pouvez demander le nom de la bibliothèque. CloudFormation ajoute ensuite la bibliothèque au package de déploiement qu'elle crée pour la fonction.

Si votre fonction qu'une ressource personnalisée utilise possède une interface réseau Elastic qui lui est associée, ajoutez les ressources suivantes à la politique VPC où **`region`** est la région dans laquelle se trouve la fonction sans les tirets. Par exemple, `us-east-1` est `useast1`. Cela permettra à la ressource personnalisée de répondre à l'URL de rappel qui renvoie un signal à la CloudFormation pile.

```
arn:aws:s3:::cloudformation-custom-resource-response-region",
"arn:aws:s3:::cloudformation-custom-resource-response-region/*",
```

L'exemple de fonction suivant appelle une deuxième fonction. Si l'appel aboutit, la fonction envoie une réponse de confirmation à CloudFormation, et la mise à jour de la pile se poursuit. Le modèle utilise le type de ressource AWS::Serverless::Function fourni par AWS Serverless Application Model.

Example– Fonction de ressource personnalisée

```
Transform: 'AWS::Serverless-2016-10-31'
Resources:
  primer:
    Type: AWS::Serverless::Function
    Properties:
      Handler: index.handler
      Runtime: nodejs16.x
      InlineCode: |
        var aws = require('aws-sdk');
        var response = require('cfn-response');
        exports.handler = function(event, context) {
            // For Delete requests, immediately send a SUCCESS response.
            if (event.RequestType == "Delete") {
                response.send(event, context, "SUCCESS");
                return;
            }
            var responseStatus = "FAILED";
            var responseData = {};
            var functionName = event.ResourceProperties.FunctionName
            var lambda = new aws.Lambda();
            lambda.invoke({ FunctionName: functionName }, function(err, invokeResult) {
                if (err) {
                    responseData = {Error: "Invoke call failed"};
                    console.log(responseData.Error + ":\n", err);
                }
                else responseStatus = "SUCCESS";
                response.send(event, context, responseStatus, responseData);
            });
        };
      Description: Invoke a function to create a log stream.
      MemorySize: 128
      Timeout: 8
      Role: !GetAtt role.Arn
      Tracing: Active
```

Si la fonction invoquée par la ressource personnalisée n'est pas définie dans un modèle, vous pouvez obtenir le code source à `cfn-response` partir du module cfn-response dans le guide de l' AWS CloudFormation utilisateur.

Pour plus d’informations sur les ressources personnalisées, consultez Ressources personnalisées dans le Guide de l’utilisateur AWS CloudFormation .

Traiter les événements Amazon DocumentDB avec Lambda

Vous pouvez utiliser une fonction d'événement Lambda pour traiter les événements d'un flux de modifications Amazon DocumentDB (compatible avec MongoDB) en configurant un cluster Amazon DocumentDB comme source d'événements. Vous pouvez ensuite automatiser les charges de travail pilotées par les événements en invoquant votre fonction d'événement Lambda chaque fois que les données sont modifiées dans votre cluster Amazon DocumentDB.

> **Note**
>
> Lambda prend en charge uniquement les versions 4.0 et 5.0 d'Amazon DocumentDB. Lambda ne prend pas en charge la version 3.6.
> De plus, pour les mappages des sources d'événements, Lambda ne prend en charge que les clusters basés sur des instances et les clusters régionaux. Lambda ne prend pas en charge les clusters élastiques ni les clusters globaux. Cette limitation ne s'applique pas lorsque vous utilisez Lambda en tant que client pour vous connecter à Amazon DocumentDB. Lambda peut se connecter à tous les types de clusters pour effectuer des opérations CRUD.

Lambda traite les événements des flux de modifications Amazon DocumentDB de manière séquentielle dans l'ordre de leur arrivée. Pour cette raison, votre fonction ne peut gérer qu'une seule invocation simultanée d'Amazon DocumentDB à la fois. Pour surveiller votre fonction, vous pouvez suivre ses métriques de simultanéité.

> **Warning**
>
> Les mappages des sources d'événements Lambda traitent chaque événement au moins une fois, et le traitement des enregistrements peut être dupliqué. Pour éviter les problèmes potentiels liés à des événements dupliqués, nous vous recommandons vivement de rendre votre code de fonction idempotent. Pour en savoir plus, consultez Comment rendre ma fonction Lambda idempotente dans le Knowledge Center. AWS

Rubriques

- Exemple d'événement Amazon DocumentDB
- Conditions préalables et autorisations
- Configurer la sécurité réseau

- Création d'un mappage des sources d'événements Amazon DocumentDB (console)
- Création d'un mappage des sources d'événements Amazon DocumentDB (kit SDK ou CLI)
- Positions de départ des interrogations et des flux
- Surveillance de votre source d'événements Amazon DocumentDB
- Tutoriel : Utilisation AWS Lambda avec Amazon DocumentDB Streams

Exemple d'événement Amazon DocumentDB


```
{
    "eventSourceArn": "arn:aws:rds:us-
east-1:123456789012:cluster:canaryclusterb2a659a2-qo5tcmqkcl03",
    "events": [
        {
            "event": {
                "_id": {
                    "_data": "0163eeb6e7000000090100000009000041e1"
                },
                "clusterTime": {
                    "$timestamp": {
                        "t": 1676588775,
                        "i": 9
                    }
                },
                "documentKey": {
                    "_id": {
                        "$oid": "63eeb6e7d418cd98afb1c1d7"
                    }
                },
                "fullDocument": {
                    "_id": {
                        "$oid": "63eeb6e7d418cd98afb1c1d7"
                    },
                    "anyField": "sampleValue"
                },
                "ns": {
                    "db": "test_database",
                    "coll": "test_collection"
                },
                "operationType": "insert"
            }
        }
```

```
    ],
    "eventSource": "aws:docdb"
}
```

Pour plus d'informations sur les événements de cet exemple et leurs formes, consultez la page Événements de modification sur le site Web de la documentation MongoDB.

Conditions préalables et autorisations

Avant de pouvoir utiliser Amazon DocumentDB comme source d'événements pour votre fonction d'événement Lambda, tenez compte des conditions préalables suivantes. Vous devez :

- Disposez d'un cluster Amazon DocumentDB existant dans le même Compte AWS cluster Région AWS que votre fonction. Si vous n'avez pas de cluster existant, vous pouvez en créer un en suivant les étapes de la section Prise en main d'Amazon DocumentDB dans le Guide du développeur Amazon DocumentDB. Sinon, la première série d'étapes de Tutoriel : Utilisation AWS Lambda avec Amazon DocumentDB Streams vous guide dans la création d'un cluster Amazon DocumentDB avec tous les prérequis nécessaires.
- Autorisez Lambda à accéder aux ressources Amazon Virtual Private Cloud (Amazon VPC) associées à votre cluster Amazon DocumentDB. Pour plus d'informations, consultez Configurer la sécurité réseau.
- Activez le protocole TLS sur votre cluster Amazon DocumentDB. Il s'agit du paramètre par défaut. Si vous désactivez le protocole TLS, Lambda ne peut pas communiquer avec votre cluster.
- Activez les flux de modifications sur votre cluster Amazon DocumentDB. Pour plus d'informations, veuillez consulter la rubrique Utilisation des flux de modifications avec Amazon DocumentDB dans le Guide du développeur Amazon DocumentDB.
- Fournissez à Lambda les informations d'identification pour accéder à votre cluster Amazon DocumentDB. Lors de la configuration de la source d'événement, fournissez la clé AWS Secrets Manager qui contient les informations d'authentification (nom d'utilisateur et mot de passe) requises pour accéder à votre cluster. Pour fournir cette clé lors de la configuration, procédez de l'une des manières suivantes :
  - Si vous utilisez la console Lambda pour la configuration, saisissez cette clé dans le champ Clé du gestionnaire de secrets.
  - Si vous utilisez le AWS Command Line Interface (AWS CLI) pour la configuration, fournissez cette clé dans l'`source-access-configuration`option. Vous pouvez inclure cette option avec la commande `create-event-source-mapping` ou la commande `update-event-source-mapping`. Par exemple :

```
aws lambda create-event-source-mapping \
    ...
    --source-access-configurations
 '[{"Type":"BASIC_AUTH","URI":"arn:aws:secretsmanager:us-
west-2:123456789012:secret:DocDBSecret-AbC4E6"}]' \
    ...
```

- Accordez des autorisations à Lambda pour gérer les ressources liées à votre flux Amazon DocumentDB. Ajoutez manuellement les autorisations suivantes au rôle d'exécution de votre fonction :
  - rds:DescribeDBClusters
  - rouge : DescribeDBClusterParameters
  - rouge : DescribeDBSubnetGroups
  - EC2 : CreateNetworkInterface
  - EC2 : DescribeNetworkInterfaces
  - EC2 : DescribeVpcs
  - EC2 : DeleteNetworkInterface
  - EC2 : DescribeSubnets
  - EC2 : DescribeSecurityGroups
  - kms:Decrypt
  - responsable des secrets : GetSecretValue
- La taille des événements de flux de modifications Amazon DocumentDB que vous envoyez à Lambda doit être inférieure à 6 Mo. Lambda prend en charge des charges utiles d'une taille maximale de 6 Mo. Si votre flux de modifications essaie d'envoyer à Lambda un événement supérieur à 6 Mo, Lambda supprime le message et émet la métrique `OversizedRecordCount`. Lambda émet toutes les métriques dans la mesure du possible.

> **Note**
>
> Alors que les fonctions d'événement Lambda ont généralement un délai d'expiration maximal de 15 minutes, les mappages de sources d'événements pour Amazon MSK, Apache Kafka autogéré, Amazon DocumentDB et Amazon MQ pour ActiveMQ et RabbitMQ ne prennent en charge que les fonctions dont le délai d'expiration maximal est de 14 minutes. Cette

contrainte garantit que le mappage des sources d'événements peut gérer correctement les erreurs de fonction et effectuer de nouvelles tentatives.

Configurer la sécurité réseau

Pour donner à Lambda un accès complet à Amazon DocumentDB via votre mappage des sources d'événements, soit votre cluster doit utiliser un point de terminaison public (adresse IP publique), soit vous devez fournir un accès au VPC Amazon dans lequel vous avez créé le cluster.

Lorsque vous utilisez Amazon DocumentDB avec Lambda, créez des points de terminaison AWS PrivateLink VPC qui permettent à votre fonction d'événement d'accéder aux ressources de votre Amazon VPC.

> **Note**
>
> AWS PrivateLink Les points de terminaison VPC sont requis pour les fonctions avec des mappages de sources d'événements qui utilisent le mode par défaut (à la demande) pour les sondeurs d'événements. Si le mappage de votre source d'événements utilise le mode provisionné, vous n'avez pas besoin de configurer les points de terminaison AWS PrivateLink VPC.

Créez un point de terminaison pour accéder aux ressources suivantes :

- Lambda — Créez un point de terminaison pour le principal de service Lambda.
- AWS STS — Créez un point de terminaison pour le AWS STS afin qu'un directeur de service assume un rôle en votre nom.
- Secrets Manager : si votre cluster utilise Secrets Manager pour stocker les informations d'identification, créez un point de terminaison pour Secrets Manager.

Vous pouvez également configurer une passerelle NAT sur chaque sous-réseau public d'Amazon VPC. Pour plus d'informations, consultez the section called "Accès Internet pour les fonctions VPC".

Lorsque vous créez un mappage des sources d'événements pour Amazon DocumentDB, Lambda vérifie si des interfaces réseau Elastic (ENI) sont déjà présentes pour les sous-réseaux et les groupes de sécurité configurés pour votre VPC Amazon. Si Lambda trouve des ENI existantes, il tente de

les réutiliser. Sinon, Lambda crée de nouvelles ENI pour se connecter à la source d'événement et invoquer votre fonction.

> **Note**
>
> Les fonctions d'événement Lambda s'exécutent toujours dans des VPC appartenant au service Lambda. La configuration VPC de votre fonction n'affecte pas le mappage des sources d'événements. Seule la configuration réseau des sources d'événements détermine la manière dont Lambda se connecte à votre source d'événements.

Configurez les groupes de sécurité pour le VPC Amazon contenant votre cluster. Par défaut, Amazon DocumentDB utilise les ports suivants : `27017`.

- Règles entrantes – Autorisent tout le trafic sur le port de l'agent par défaut pour le groupe de sécurité associé à votre source d'événement. Vous pouvez également utiliser une règle de groupe de sécurité avec référence circulaire pour autoriser l'accès à partir d'instances appartenant au même groupe de sécurité.
- Règles de sortie : autorisez tout le trafic sur le port `443` pour les destinations externes si votre fonction doit communiquer avec les AWS services. Vous pouvez également utiliser une règle de groupe de sécurité à référencement automatique pour limiter l'accès au courtier si vous n'avez pas besoin de communiquer avec d'autres AWS services.
- Règles entrantes relatives au point de terminaison Amazon VPC – Si vous utilisez un point de terminaison Amazon VPC, le groupe de sécurité associé à votre point de terminaison Amazon VPC doit autoriser le trafic entrant sur le port `443` en provenance du groupe de sécurité du cluster.

Si votre cluster utilise l'authentification, vous pouvez également restreindre la politique de point de terminaison pour le point de terminaison Secrets Manager. Pour appeler l'API Secrets Manager, Lambda utilise votre rôle de fonction, et non le principal de service Lambda.

Example Politique de point de terminaison de VPC — Point de terminaison Secrets Manager

```
{
      "Statement": [
          {
              "Action": "secretsmanager:GetSecretValue",
              "Effect": "Allow",
              "Principal": {
```

```
                "AWS": [
                    "arn:aws::iam::123456789012:role/my-role"
                ]
            },
            "Resource": "arn:aws::secretsmanager:us-west-2:123456789012:secret:my-
secret"
        }
    ]
}
```

Lorsque vous utilisez des points de terminaison Amazon VPC, AWS achemine vos appels d'API pour appeler votre fonction à l'aide de l'Elastic Network Interface (ENI) du point de terminaison. Le principal de service Lambda doit appeler `lambda:InvokeFunction` pour tous les rôles et fonctions utilisant ces ENI.

Par défaut, les points de terminaison Amazon VPC disposent de politiques IAM ouvertes qui permettent un accès étendu aux ressources. La meilleure pratique consiste à restreindre ces politiques pour effectuer les actions nécessaires à l'aide de ce point de terminaison. Pour garantir que le mappage de votre source d'événements est en mesure d'appeler votre fonction d'événement Lambda, la politique de point de terminaison VPC doit autoriser le principal du service Lambda à appeler et. `sts:AssumeRole` `lambda:InvokeFunction` Le fait de restreindre vos politiques de point de terminaison de VPC pour autoriser uniquement les appels d'API provenant de votre organisation empêche le mappage des sources d'événements de fonctionner correctement. C'est pourquoi `"Resource": "*"` est requis dans ces politiques.

Les exemples de politiques de point de terminaison de VPC suivants montrent comment accorder l'accès requis au principal de service Lambda pour les points de terminaison AWS STS et Lambda.

Example Politique relative aux points de terminaison VPC — AWS STS point de terminaison

```
{
    "Statement": [
        {
            "Action": "sts:AssumeRole",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "lambda.amazonaws.com"
                ]
            },
            "Resource": "*"
```

```
            }
        ]
    }
```

Example Politique de point de terminaison de VPC — Point de terminaison Lambda

```
{
      "Statement": [
          {
              "Action": "lambda:InvokeFunction",
              "Effect": "Allow",
              "Principal": {
                  "Service": [
                      "lambda.amazonaws.com"
                  ]
              },
              "Resource": "*"
          }
      ]
  }
```

Création d’un mappage des sources d’événements Amazon DocumentDB (console)

Pour qu'une fonction d'événement Lambda puisse lire le flux de modifications d'un cluster Amazon DocumentDB, créez un mappage des sources d'événements. Cette section explique comment procéder à partir de la console Lambda. Pour le AWS SDK et les AWS CLI instructions, voirthe section called “Création d’un mappage des sources d’événements Amazon DocumentDB (kit SDK ou CLI)”.

Pour créer un mappage des sources d’événements Amazon DocumentDB (console)

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez le nom d’une fonction.
3. Sous Function overview (Présentation de la fonction), choisissez Add trigger (Ajouter un déclencheur).
4. Sous Configuration du déclencheur, dans la liste déroulante, choisissez DocumentDB.
5. Configurez les options requises, puis choisissez Add (Ajouter).

Lambda prend en charge les options suivantes pour les sources d'événement Amazon DocumentDB :

- Cluster DocumentDB : sélectionnez un cluster Amazon DocumentDB.
- Activer le déclencheur : choisissez si vous voulez activer le déclencheur maintenant. Si vous cochez cette case, votre fonction commence immédiatement à recevoir du trafic provenant du flux de modifications Amazon DocumentDB spécifié lors de la création du mappage des sources d'événements. Nous vous recommandons de décocher la case pour créer le mappage des sources d'événements dans un état désactivé à des fins de test. Après la création, vous pouvez activer le mappage des sources d'événements à tout moment.
- Nom de la base de données – Saisissez le nom de la base de données du cluster à utiliser.
- (Facultatif) Nom de la collection : saisissez le nom d'une collection de la base de données à utiliser. Si vous n'indiquez pas de collection, Lambda écoute tous les événements de chaque collection de la base de données.
- Taille de lot – Définissez le nombre maximum de messages à extraire dans un lot, jusqu'à 10 000. La taille du lot par défaut est de 100.
- Position de départ – Choisissez la position dans le flux à partir de laquelle commencer la lecture des enregistrements.
  - Derniers – Traiter uniquement les nouveaux enregistrements qui sont ajoutés au flux. Votre fonction ne commence à traiter les enregistrements que lorsque Lambda a fini de créer votre source d'événements. Cela signifie que certains enregistrements peuvent être supprimés jusqu'à ce que votre source d'événements soit créée avec succès.
  - Trim horizon (Supprimer l'horizon) – Traiter tous les enregistrements figurant dans le flux. Lambda utilise la durée de conservation des journaux de votre cluster pour déterminer par où commencer la lecture des événements. Plus précisément, Lambda commence à lire à partir de `current_time - log_retention_duration`. Votre flux de modifications doit déjà être actif avant cet horodatage pour que Lambda puisse lire correctement tous les événements.
  - At timestamp (À l'horodatage) – Traitez les enregistrements à partir d'une heure spécifique. Votre flux de modifications doit déjà être actif avant l'horodatage spécifié pour que Lambda puisse lire correctement tous les événements.
- Authentication – Choisissez la méthode d'authentification pour accéder aux agents de votre cluster.
  - BASIC_AUTH – Avec l'authentification de base, vous devez fournir la clé Secrets Manager qui contient les informations d'identification pour accéder à votre cluster.

- Clé Secrets Manager : choisissez la clé Secrets Manager qui contient les informations d'authentification (nom d'utilisateur et mot de passe) requises pour accéder à votre cluster Amazon DocumentDB.
- (Facultatif) Fenêtre de traitement par lot : définissez l'intervalle de temps maximum (en secondes) pour collecter des enregistrements avant d'invoquer votre fonction, jusqu'à 300.
- (Facultatif) Configuration complète du document : pour les opérations de mise à jour des documents, choisissez ce que vous voulez envoyer au flux. La valeur par défaut est `Default`, ce qui signifie que pour chaque événement de flux de modifications, Amazon DocumentDB envoie uniquement un delta décrivant les modifications apportées. Pour plus d'informations sur ce champ, consultez la documentation FullDocumentde l'API MongoDB Javadoc.
  - Par défaut – Lambda n'envoie qu'un document partiel décrivant les modifications apportées.
  - UpdateLookup— Lambda envoie un delta décrivant les modifications, ainsi qu'une copie de l'intégralité du document.

Création d'un mappage des sources d'événements Amazon DocumentDB (kit SDK ou CLI)

Pour créer ou gérer votre mappage des sources d'événements Amazon DocumentDB avec un kit SDK AWS, vous pouvez utiliser les opérations d'API suivantes :

- CreateEventSourceMapping
- ListEventSourceMappings
- GetEventSourceMapping
- UpdateEventSourceMapping
- DeleteEventSourceMapping

Pour créer le mappage des sources d'événements avec le AWS CLI, utilisez la `create-event-source-mapping`commande. L'exemple suivant utilise cette commande pour mapper une fonction nommée `my-function` à un flux de modifications Amazon DocumentDB. La source d'événement est spécifiée par un Amazon Resource Name (ARN), avec une taille de lot de 500, à partir de l'horodatage en heure Unix. La commande spécifie également la clé Secrets Manager que Lambda utilise pour se connecter à Amazon DocumentDB. De plus, elle inclut des paramètres `document-db-event-source-config` qui spécifient la base de données et la collection à partir de laquelle lire.

```
aws lambda create-event-source-mapping --function-name my-function \
    --event-source-arn arn:aws:rds:us-west-2:123456789012:cluster:privatecluster7de2-
epzcyvu4pjoy
    --batch-size 500 \
    --starting-position AT_TIMESTAMP \
    --starting-position-timestamp 1541139109 \
    --source-access-configurations
 '[{"Type":"BASIC_AUTH","URI":"arn:aws:secretsmanager:us-
east-1:123456789012:secret:DocDBSecret-BAtjxi"}]' \
    --document-db-event-source-config '{"DatabaseName":"test_database",
 "CollectionName": "test_collection"}' \
```

Vous devriez obtenir un résultat du type suivant :

```
{
    "UUID": "2b733gdc-8ac3-cdf5-af3a-1827b3b11284",
    "BatchSize": 500,
    "DocumentDBEventSourceConfig": {
        "CollectionName": "test_collection",
        "DatabaseName": "test_database",
        "FullDocument": "Default"
    },
    "MaximumBatchingWindowInSeconds": 0,
    "EventSourceArn": "arn:aws:rds:us-west-2:123456789012:cluster:privatecluster7de2-
epzcyvu4pjoy",
    "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-function",
    "LastModified": 1541348195.412,
    "LastProcessingResult": "No records processed",
    "State": "Creating",
    "StateTransitionReason": "User action"
}
```

Après la création, vous pouvez utiliser la commande `update-event-source-mapping` pour mettre à jour les paramètres de votre source d'événements Amazon DocumentDB. L'exemple suivant met à jour la taille du lot à 1 000 et la fenêtre de traitement par lots à 10 secondes. Pour cette commande, vous avez besoin de l'UUID de votre mappage des sources d'événements, que vous pouvez récupérer à l'aide de la commande `list-event-source-mapping` ou de la console Lambda.

```
aws lambda update-event-source-mapping --function-name my-function \
    --uuid f89f8514-cdd9-4602-9e1f-01a5b77d449b \
```

```
    --batch-size 1000 \
    --batch-window 10
```

Vous devriez obtenir un résultat du type suivant :

```
{
    "UUID": "2b733gdc-8ac3-cdf5-af3a-1827b3b11284",
    "BatchSize": 500,
    "DocumentDBEventSourceConfig": {
        "CollectionName": "test_collection",
        "DatabaseName": "test_database",
        "FullDocument": "Default"
    },
    "MaximumBatchingWindowInSeconds": 0,
    "EventSourceArn": "arn:aws:rds:us-west-2:123456789012:cluster:privatecluster7de2-
epzcyvu4pjoy",
    "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-function",
    "LastModified": 1541359182.919,
    "LastProcessingResult": "OK",
    "State": "Updating",
    "StateTransitionReason": "User action"
}
```

Lambda met à jour les paramètres de manière asynchrone, il est donc possible que vous ne voyiez pas ces modifications dans la sortie tant que le processus n'est pas terminé. Pour afficher les paramètres actuels de votre mappage des sources d'événements, utilisez la commande `get-event-source-mapping`.

```
aws lambda get-event-source-mapping --uuid f89f8514-cdd9-4602-9e1f-01a5b77d449b
```

Vous devriez obtenir un résultat du type suivant :

```
{
    "UUID": "2b733gdc-8ac3-cdf5-af3a-1827b3b11284",
    "DocumentDBEventSourceConfig": {
        "CollectionName": "test_collection",
        "DatabaseName": "test_database",
        "FullDocument": "Default"
    },
    "BatchSize": 1000,
    "MaximumBatchingWindowInSeconds": 10,
```

```
    "EventSourceArn": "arn:aws:rds:us-west-2:123456789012:cluster:privatecluster7de2-
epzcyvu4pjoy",
    "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-function",
    "LastModified": 1541359182.919,
    "LastProcessingResult": "OK",
    "State": "Enabled",
    "StateTransitionReason": "User action"
}
```

Pour supprimer le mappage des sources d'événements Amazon DocumentDB, utilisez la commande `delete-event-source-mapping`.

```
aws lambda delete-event-source-mapping \
    --uuid 2b733gdc-8ac3-cdf5-af3a-1827b3b11284
```

Positions de départ des interrogations et des flux

Sachez que l'interrogation des flux lors des mises à jour et de la création du mappage des sources d'événements est finalement cohérente.

- Lors de la création du mappage des sources d'événements, le démarrage de l'interrogation des événements depuis le flux peut prendre plusieurs minutes.
- Lors des mises à jour du mappage des sources d'événements, l'arrêt et le redémarrage de l'interrogation des événements depuis le flux peuvent prendre plusieurs minutes.

Ce comportement signifie que si vous spécifiez `LATEST` comme position de départ du flux, le mappage des sources d'événements peut manquer des événements lors de la création ou des mises à jour. Pour vous assurer de ne manquer aucun événement, spécifiez la position de départ du flux comme `TRIM_HORIZON` ou `AT_TIMESTAMP`.

Surveillance de votre source d'événements Amazon DocumentDB

Pour vous aider à surveiller votre source d'événements Amazon DocumentDB, Lambda émet la métrique `IteratorAge` lorsque votre fonction termine le traitement d'un lot d'enregistrements. L'âge de l'itérateur est la différence entre l'horodatage de l'événement le plus récent et l'horodatage actuel. La métrique `IteratorAge` indique essentiellement l'ancienneté du dernier enregistrement traité dans le lot.

Si votre fonction traite actuellement de nouveaux événements, vous pouvez utiliser l'âge de l'itérateur pour estimer la latence entre le moment où un enregistrement est ajouté et celui où votre fonction le

traite. Une tendance à la hausse de `IteratorAge` peut indiquer des problèmes liés à votre fonction. Pour plus d'informations, consultez Utilisation de CloudWatch métriques avec Lambda.

Les flux de modifications Amazon DocumentDB ne sont pas optimisés pour gérer les intervalles de temps importants entre les événements. Si votre source d'événements Amazon DocumentDB ne reçoit aucun événement pendant une période prolongée, Lambda peut désactiver le mappage de la source d'événements. Cette période peut varier de quelques semaines à quelques mois en fonction de la taille du cluster et des autres charges de travail.

Lambda prend en charge des charges utiles allant jusqu'à 6 Mo. Cependant, les événements du flux de modification d'Amazon DocumentDB peuvent avoir une taille allant jusqu'à 16 Mo. Si votre flux de modifications tente d'envoyer à Lambda un événement d'une taille supérieure à 6 Mo, Lambda supprime le message et émet la métrique `OversizedRecordCount`. Lambda émet toutes les métriques dans la mesure du possible.

Tutoriel : Utilisation AWS Lambda avec Amazon DocumentDB Streams

Dans ce didacticiel, vous allez créer une fonction d'événement Lambda de base qui utilise les événements d'un flux de modifications d'Amazon DocumentDB (compatible avec MongoDB). Pour terminer ce didacticiel, vous devez suivre les étapes suivantes :

- Configurez votre cluster Amazon DocumentDB, connectez-vous-y, et activez les flux de modifications sur ce cluster.
- Créez votre fonction d'événement Lambda et configurez votre cluster Amazon DocumentDB en tant que source d'événements pour votre fonction.
- Testez la configuration en insérant des éléments dans votre base de données Amazon DocumentDB.

Créer le cluster Amazon DocumentDB

1. Ouvrez la console Amazon DocumentDB. Sous Clusters, sélectionnez Créer.
2. Créez un cluster avec la configuration suivante :
   - Pour Type de cluster, choisissez Instance-based cluster. Il s'agit de l'option par défaut.
   - Sous Configuration du cluster, assurez-vous que la Version du moteur 5.0.0 est sélectionnée. Il s'agit de l'option par défaut.
   - Sous Configuration de l'instance :

    - Pour Classe d’instance de base de données, sélectionnez Classes à mémoire optimisée. Il s’agit de l’option par défaut.
    - Pour Nombre d’instances de réplica ordinaire, choisissez 1.
    - Pour Classe de l’instance, utilisez la sélection par défaut.
  - Sous Authentification, saisissez un nom d’utilisateur pour l’utilisateur principal, puis choisissez Autogéré. Saisissez un mot de passe, puis confirmez-le.
  - Conservez tous les autres paramètres par défaut.
3. Choisissez Créer un cluster.

Création d’un secret dans Secrets Manager

Pendant qu'Amazon DocumentDB crée votre cluster, créez un AWS Secrets Manager secret pour stocker les informations d'identification de votre base de données. Vous fournirez ce secret lors de la création du mappage des sources d’événements Lambda lors d’une étape ultérieure.

Pour créer le secret dans Secrets Manager

1. Ouvrez la console Secrets Manager et choisissez Stocker un nouveau secret.
2. Pour Choisir le type de secret, sélectionnez les options suivantes :
    - Sous Informations de base :
      - Type de secret : informations d’identification pour votre base de données Amazon DocumentDB
      - Sous Informations d’identification, saisissez les mêmes nom d’utilisateur et mot de passe que vous avez utilisés pour créer votre cluster Amazon DocumentDB.
      - Base de données : choisissez votre cluster Amazon DocumentDB.
      - Choisissez Suivant.
3. Pour Configurer le secret, choisissez les options suivantes :
    - Nom secret : `DocumentDBSecret`
    - Choisissez Suivant.
4. Choisissez Suivant.
5. Choisissez Stocker.
6. Actualisez la console pour vérifier que vous avez correctement enregistré le secret `DocumentDBSecret`.

Notez l'ARN du secret. Vous en aurez besoin ultérieurement.

Connexion au cluster

Connectez-vous à votre cluster Amazon DocumentDB à l'aide de AWS CloudShell

1. Dans la console de gestion Amazon DocumentDB, sous Clusters, recherchez le cluster que vous avez créé. Choisissez votre cluster en cochant la case à côté de celui-ci.
2. Choisissez Se connecter au cluster. L'écran CloudShell Exécuter la commande apparaît.
3. Dans le champ Nom du nouvel environnement, saisissez un nom unique, comme « test », puis choisissez Créer et exécuter.
4. Lorsque vous y êtes invité, saisissez votre mot de passe. Lorsque l'invite affiche `rs0 [direct: primary] <env-name>>`, vous êtes connecté avec succès à votre cluster Amazon DocumentDB.

Activation des flux de modifications

Dans le cadre de ce didacticiel, vous allez suivre les modifications apportées à la `products` collection de la `docdbdemo` base de données dans votre cluster Amazon DocumentDB. Pour ce faire, vous activez les flux de modifications.

Pour créer une nouvelle base de données dans votre cluster

1. Exécutez la commande suivante pour créer une nouvelle base de données appelée `docdbdemo` :

   ```
   use docdbdemo
   ```

2. Dans la fenêtre de terminal, utilisez la commande suivante pour insérer un enregistrement dans `docdbdemo` :

   ```
   db.products.insertOne({"hello":"world"})
   ```

   Elle doit générer une sortie comme suit :

   ```
   {
     acknowledged: true,
     insertedId: ObjectId('67f85066ca526410fd531d59')
   ```

```
}
```

3. Activez ensuite les flux de modifications sur la collection `products` de la base de données `docdbdemo` à l'aide de la commande suivante :

```
db.adminCommand({modifyChangeStreams: 1,
    database: "docdbdemo",
    collection: "products",
    enable: true});
```

Vous devriez obtenir un résultat du type suivant :

```
{ "ok" : 1, "operationTime" : Timestamp(1680126165, 1) }
```

Création de points de terminaison d'un VPC d'interface

Créez ensuite des points de terminaison d'un VPC d'interface pour vous assurer que Lambda et Secrets Manager (utilisé plus tard pour stocker nos informations d'identification d'accès au cluster) peuvent se connecter à votre VPC par défaut.

Pour créer des points de terminaison d'un VPC d'interface

1. Ouvrez la console VPC. Dans le menu de gauche, sous Cloud privé virtuel, choisissez Points de terminaison.
2. Choisissez Créer un point de terminaison. Créez un point de terminaison avec la configuration suivante :
   - Pour Balise de nom, saisissez `lambda-default-vpc`.
   - Pour la catégorie de service, sélectionnez AWS services.
   - Pour Services, saisissez `lambda` dans la zone de recherche. Choisissez le service au format `com.amazonaws.<region>.lambda`.
   - Pour VPC, choisissez le VPC dans lequel se trouve votre cluster Amazon DocumentDB. Il s'agit généralement du VPC par défaut.
   - Pour Sous-réseaux, cochez les cases à côté de chaque zone de disponibilité. Choisissez l'ID de sous-réseau correct pour chaque zone de disponibilité.
   - Pour Type d'adresse IP, sélectionnez IPv4.

- Pour Groupes de sécurité, choisissez le groupe de sécurité utilisé par votre cluster Amazon DocumentDB. Il s'agit généralement du groupe de sécurité `default`.
- Conservez tous les autres paramètres par défaut.
- Choisissez Créer un point de terminaison.

3. Choisissez à nouveau Créer un point de terminaison. Créez un point de terminaison avec la configuration suivante :

   - Pour Balise de nom, saisissez `secretsmanager-default-vpc`.
   - Pour la catégorie de service, sélectionnez AWS services.
   - Pour Services, saisissez `secretsmanager` dans la zone de recherche. Choisissez le service au format `com.amazonaws.<region>.secretsmanager`.
   - Pour VPC, choisissez le VPC dans lequel se trouve votre cluster Amazon DocumentDB. Il s'agit généralement du VPC par défaut.
   - Pour Sous-réseaux, cochez les cases à côté de chaque zone de disponibilité. Choisissez l'ID de sous-réseau correct pour chaque zone de disponibilité.
   - Pour Type d'adresse IP, sélectionnez IPv4.
   - Pour Groupes de sécurité, choisissez le groupe de sécurité utilisé par votre cluster Amazon DocumentDB. Il s'agit généralement du groupe de sécurité `default`.
   - Conservez tous les autres paramètres par défaut.
   - Choisissez Créer un point de terminaison.

Ceci termine la partie de ce tutoriel concernant la configuration du cluster.

Créer le rôle d'exécution

Au cours des étapes suivantes, vous allez créer votre fonction d'événement Lambda. Tout d'abord, vous devez créer le rôle d'exécution qui donne à votre fonction l'autorisation d'accéder à votre cluster. Vous faites cela en créant d'abord une politique IAM, puis en associant cette politique à un rôle IAM.

Pour créer une politique IAM

1. Ouvrez la page Politiques dans la console IAM et choisissez Créer une politique.

2. Choisissez l’onglet JSON. Dans la politique suivante, remplacez l'ARN de la ressource Secrets Manager dans la dernière ligne de l'instruction par votre ARN secret précédent et copiez la politique dans l'éditeur.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "LambdaESMNetworkingAccess",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeVpcs",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups",
                "kms:Decrypt"
            ],
            "Resource": "*"
        },
        {
            "Sid": "LambdaDocDBESMAccess",
            "Effect": "Allow",
            "Action": [
                "rds:DescribeDBClusters",
                "rds:DescribeDBClusterParameters",
                "rds:DescribeDBSubnetGroups"
            ],
            "Resource": "*"
        },
        {
            "Sid": "LambdaDocDBESMGetSecretValueAccess",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": "arn:aws:secretsmanager:us-
east-1:123456789012:secret:DocumentDBSecret"
        }
```

```
    ]
}
```

3. Choisissez Suivant : Balises, puis Suivant : Vérification.
4. Pour Nom, saisissez `AWSDocumentDBLambdaPolicy`.
5. Sélectionnez Create policy (Créer une politique).

Pour créer le rôle IAM

1. Ouvrez la page Rôles dans la console IAM et choisissez Créer un rôle.
2. Pour Sélectionner une entité de confiance, choisissez les options suivantes :
   - Type d'entité de confiance : AWS service
   - Service ou cas d’utilisation : Lambda
   - Choisissez Suivant.
3. Pour Ajouter des autorisations, choisissez la `AWSDocumentDBLambdaPolicy` politique que vous venez de créer, ainsi que celle permettant `AWSLambdaBasicExecutionRole` à votre fonction d'écrire sur Amazon CloudWatch Logs.
4. Choisissez Suivant.
5. Pour le Nom du rôle, saisissez `AWSDocumentDBLambdaExecutionRole`.
6. Choisissez Créer un rôle.

Création de la fonction d'événement Lambda

Ce didacticiel utilise le moteur d'exécution Python 3.14, mais nous avons également fourni des exemples de fichiers de code pour d'autres environnements d'exécution. Vous pouvez sélectionner l'onglet dans la zone suivante pour voir le code du moteur d'exécution qui vous intéresse.

Le code reçoit une entrée d’événement Amazon DocumentDB et traite le message qu’elle contient.

Pour créer la fonction d'événement Lambda

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez Create Event Function.
3. Choisissez Créer à partir de zéro.
4. Sous Basic information (Informations de base), procédez comme suit :

a. Sous Nom de la fonction, saisissez `ProcessDocumentDBRecords`.

b. Pour Runtime, choisissez Python 3.14.

c. Pour Architecture, choisissez x86_64.

5. Dans l'onglet Modifier le rôle d'exécution par défaut, procédez comme suit :

a. Ouvrez l'onglet, puis choisissez Utiliser un rôle existant.

b. Sélectionnez le `AWSDocumentDBLambdaExecutionRole` que vous avez créé précédemment.

6. Choisissez Create Event Function.

Pour déployer le code de la fonction d'événement

1. Choisissez l'onglet Python dans la zone suivante et copiez le code.

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement Amazon DocumentDB avec Lambda en utilisant .NET.

```
using Amazon.Lambda.Core;
using System.Text.Json;
using System;
using System.Collections.Generic;
using System.Text.Json.Serialization;
//Assembly attribute to enable the Lambda function's JSON input to be
 converted into a .NET class.
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJson

namespace LambdaDocDb;
```

```
public class Function
{

     /// <summary>
    /// Lambda function entry point to process Amazon DocumentDB events.
    /// </summary>
    /// <param name="event">The Amazon DocumentDB event.</param>
    /// <param name="context">The Lambda context object.</param>
    /// <returns>A string to indicate successful processing.</returns>
    public string FunctionHandler(Event evnt, ILambdaContext context)
    {

        foreach (var record in evnt.Events)
        {
            ProcessDocumentDBEvent(record, context);
        }

        return "OK";
    }

     private void ProcessDocumentDBEvent(DocumentDBEventRecord record,
 ILambdaContext context)
    {

        var eventData = record.Event;
        var operationType = eventData.OperationType;
        var databaseName = eventData.Ns.Db;
        var collectionName = eventData.Ns.Coll;
        var fullDocument = JsonSerializer.Serialize(eventData.FullDocument,
 new JsonSerializerOptions { WriteIndented = true });

        context.Logger.LogLine($"Operation type: {operationType}");
        context.Logger.LogLine($"Database: {databaseName}");
        context.Logger.LogLine($"Collection: {collectionName}");
        context.Logger.LogLine($"Full document:\n{fullDocument}");
    }



    public class Event
    {
        [JsonPropertyName("eventSourceArn")]
        public string EventSourceArn { get; set; }
```

```
        [JsonPropertyName("events")]
        public List<DocumentDBEventRecord> Events { get; set; }

        [JsonPropertyName("eventSource")]
        public string EventSource { get; set; }
    }

    public class DocumentDBEventRecord
    {
        [JsonPropertyName("event")]
        public EventData Event { get; set; }
    }

    public class EventData
    {
        [JsonPropertyName("_id")]
        public IdData Id { get; set; }

        [JsonPropertyName("clusterTime")]
        public ClusterTime ClusterTime { get; set; }

        [JsonPropertyName("documentKey")]
        public DocumentKey DocumentKey { get; set; }

        [JsonPropertyName("fullDocument")]
        public Dictionary<string, object> FullDocument { get; set; }

        [JsonPropertyName("ns")]
        public Namespace Ns { get; set; }

        [JsonPropertyName("operationType")]
        public string OperationType { get; set; }
    }

    public class IdData
    {
        [JsonPropertyName("_data")]
        public string Data { get; set; }
    }

    public class ClusterTime
    {
        [JsonPropertyName("$timestamp")]
        public Timestamp Timestamp { get; set; }
```

```
    }

    public class Timestamp
    {
        [JsonPropertyName("t")]
        public long T { get; set; }

        [JsonPropertyName("i")]
        public int I { get; set; }
    }

    public class DocumentKey
    {
        [JsonPropertyName("_id")]
        public Id Id { get; set; }
    }

    public class Id
    {
        [JsonPropertyName("$oid")]
        public string Oid { get; set; }
    }

    public class Namespace
    {
        [JsonPropertyName("db")]
        public string Db { get; set; }

        [JsonPropertyName("coll")]
        public string Coll { get; set; }
    }
}
```

Go

Kit SDK pour Go V2

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement Amazon DocumentDB avec Lambda en utilisant Go.

```
package main

import (
 "context"
 "encoding/json"
 "fmt"

 "github.com/aws/aws-lambda-go/lambda"
)

type Event struct {
 Events []Record `json:"events"`
}

type Record struct {
 Event struct {
  OperationType string `json:"operationType"`
  NS            struct {
   DB   string `json:"db"`
   Coll string `json:"coll"`
  } `json:"ns"`
  FullDocument interface{} `json:"fullDocument"`
 } `json:"event"`
}

func main() {
 lambda.Start(handler)
}
```

```
func handler(ctx context.Context, event Event) (string, error) {
 fmt.Println("Loading function")
 for _, record := range event.Events {
  logDocumentDBEvent(record)
 }

 return "OK", nil
}

func logDocumentDBEvent(record Record) {
 fmt.Printf("Operation type: %s\n", record.Event.OperationType)
 fmt.Printf("db: %s\n", record.Event.NS.DB)
 fmt.Printf("collection: %s\n", record.Event.NS.Coll)
 docBytes, _ := json.MarshalIndent(record.Event.FullDocument, "", "  ")
 fmt.Printf("Full document: %s\n", string(docBytes))
}
```

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement Amazon DocumentDB avec Lambda en utilisant Java.

```
import java.util.List;
import java.util.Map;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;

public class Example implements RequestHandler<Map<String, Object>, String> {

    @SuppressWarnings("unchecked")
    @Override
```

```
    public String handleRequest(Map<String, Object> event, Context context) {
        List<Map<String, Object>> events = (List<Map<String, Object>>)
 event.get("events");
        for (Map<String, Object> record : events) {
            Map<String, Object> eventData = (Map<String, Object>)
 record.get("event");
            processEventData(eventData);
        }

        return "OK";
    }

    @SuppressWarnings("unchecked")
    private void processEventData(Map<String, Object> eventData) {
        String operationType = (String) eventData.get("operationType");
        System.out.println("operationType: %s".formatted(operationType));

        Map<String, Object> ns = (Map<String, Object>) eventData.get("ns");

        String db = (String) ns.get("db");
        System.out.println("db: %s".formatted(db));
        String coll = (String) ns.get("coll");
        System.out.println("coll: %s".formatted(coll));

        Map<String, Object> fullDocument = (Map<String, Object>)
 eventData.get("fullDocument");
        System.out.println("fullDocument: %s".formatted(fullDocument));
    }

}
```

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement Amazon DocumentDB avec Lambda à l'aide de. JavaScript

```
console.log('Loading function');
exports.handler = async (event, context) => {
    event.events.forEach(record => {
        logDocumentDBEvent(record);
    });
    return 'OK';
};

const logDocumentDBEvent = (record) => {
    console.log('Operation type: ' + record.event.operationType);
    console.log('db: ' + record.event.ns.db);
    console.log('collection: ' + record.event.ns.coll);
    console.log('Full document:', JSON.stringify(record.event.fullDocument,
 null, 2));
};
```

Utilisation d'un événement Amazon DocumentDB avec Lambda à l'aide de TypeScript

```
import { DocumentDBEventRecord, DocumentDBEventSubscriptionContext } from
 'aws-lambda';

console.log('Loading function');

export const handler = async (
  event: DocumentDBEventSubscriptionContext,
  context: any
): Promise<string> => {
  event.events.forEach((record: DocumentDBEventRecord) => {
    logDocumentDBEvent(record);
  });
  return 'OK';
};

const logDocumentDBEvent = (record: DocumentDBEventRecord): void => {
  console.log('Operation type: ' + record.event.operationType);
  console.log('db: ' + record.event.ns.db);
```

```
  console.log('collection: ' + record.event.ns.coll);
  console.log('Full document:', JSON.stringify(record.event.fullDocument,
 null, 2));
};
```

PHP

Kit SDK pour PHP

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement Amazon DocumentDB avec Lambda en utilisant PHP.

```
<?php

require __DIR__.'/vendor/autoload.php';

use Bref\Context\Context;
use Bref\Event\Handler;

class DocumentDBEventHandler implements Handler
{
    public function handle($event, Context $context): string
    {

        $events = $event['events'] ?? [];
        foreach ($events as $record) {
            $this->logDocumentDBEvent($record['event']);
        }
        return 'OK';
    }

    private function logDocumentDBEvent($event): void
    {
        // Extract information from the event record
```

```
        $operationType = $event['operationType'] ?? 'Unknown';
        $db = $event['ns']['db'] ?? 'Unknown';
        $collection = $event['ns']['coll'] ?? 'Unknown';
        $fullDocument = $event['fullDocument'] ?? [];

        // Log the event details

        echo "Operation type: $operationType\n";
        echo "Database: $db\n";
        echo "Collection: $collection\n";
        echo "Full document: " . json_encode($fullDocument,
 JSON_PRETTY_PRINT) . "\n";
    }
}
return new DocumentDBEventHandler();
```

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement Amazon DocumentDB avec Lambda en utilisant Python.

```
import json

def lambda_handler(event, context):
    for record in event.get('events', []):
        log_document_db_event(record)
    return 'OK'

def log_document_db_event(record):
    event_data = record.get('event', {})
    operation_type = event_data.get('operationType', 'Unknown')
    db = event_data.get('ns', {}).get('db', 'Unknown')
    collection = event_data.get('ns', {}).get('coll', 'Unknown')
    full_document = event_data.get('fullDocument', {})
```

```
    print(f"Operation type: {operation_type}")
    print(f"db: {db}")
    print(f"collection: {collection}")
    print("Full document:", json.dumps(full_document, indent=2))
```

Ruby

Kit SDK pour Ruby

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement Amazon DocumentDB avec Lambda en utilisant Ruby.

```
require 'json'

def lambda_handler(event:, context:)
  event['events'].each do |record|
    log_document_db_event(record)
  end
  'OK'
end

def log_document_db_event(record)
  event_data = record['event'] || {}
  operation_type = event_data['operationType'] || 'Unknown'
  db = event_data.dig('ns', 'db') || 'Unknown'
  collection = event_data.dig('ns', 'coll') || 'Unknown'
  full_document = event_data['fullDocument'] || {}

  puts "Operation type: #{operation_type}"
  puts "db: #{db}"
  puts "collection: #{collection}"
  puts "Full document: #{JSON.pretty_generate(full_document)}"
end
```

Rust

SDK pour Rust

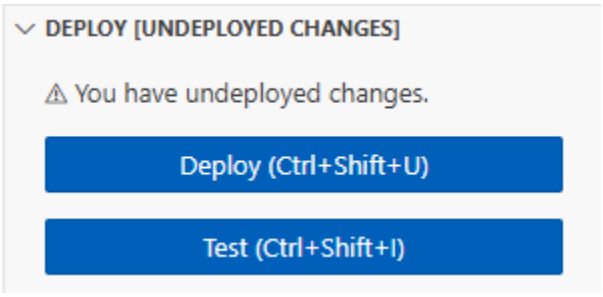
> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement Amazon DocumentDB avec Lambda en utilisant Rust.

```
use lambda_runtime::{service_fn, tracing, Error, LambdaEvent};
use aws_lambda_events::{
    event::documentdb::{DocumentDbEvent, DocumentDbInnerEvent},
   };


// Built with the following dependencies:
//lambda_runtime = "0.11.1"
//serde_json = "1.0"
//tokio = { version = "1", features = ["macros"] }
//tracing = { version = "0.1", features = ["log"] }
//tracing-subscriber = { version = "0.3", default-features = false, features
 = ["fmt"] }
//aws_lambda_events = "0.15.0"

async fn function_handler(event: LambdaEvent<DocumentDbEvent>) ->Result<(),
 Error> {

    tracing::info!("Event Source ARN: {:?}", event.payload.event_source_arn);
    tracing::info!("Event Source: {:?}", event.payload.event_source);

    let records = &event.payload.events;

    if records.is_empty() {
        tracing::info!("No records found. Exiting.");
        return Ok(());
    }
```

```
    for record in records{
        log_document_db_event(record);
    }

    tracing::info!("Document db records processed");

    // Prepare the response
    Ok(())

}

fn log_document_db_event(record: &DocumentDbInnerEvent)-> Result<(), Error>{
    tracing::info!("Change Event: {:?}", record.event);

    Ok(())

}

#[tokio::main]
async fn main() -> Result<(), Error> {
    tracing_subscriber::fmt()
    .with_max_level(tracing::Level::INFO)
    .with_target(false)
    .without_time()
    .init();

    let func = service_fn(function_handler);
    lambda_runtime::run(func).await?;
    Ok(())

}
```

2. Dans le volet Code source de la console Lambda, collez le code dans l'éditeur de code, en remplaçant le code créé par Lambda.
3. Dans la section DÉPLOYER, choisissez Déployer pour mettre à jour le code de votre fonction :



Création du mappage des sources d'événements Lambda

Créez le mappage des sources d'événements qui associe votre flux de modifications Amazon DocumentDB à votre fonction d'événement Lambda. Une fois que vous avez créé ce mappage des sources d'événements, commence AWS Lambda immédiatement à interroger le flux.

Pour créer le mappage des sources d'événements

1. Ouvrez la page Event Functions dans la console Lambda.
2. Choisissez la fonction `ProcessDocumentDBRecords` que vous avez créée précédemment.
3. Choisissez l'onglet Configuration, puis Déclencheurs dans le menu de gauche.
4. Choisissez Add trigger (Ajouter déclencheur).
5. Sous Configuration du déclencheur, pour la source, sélectionnez Amazon DocumentDB.
6. Créez le mappage des sources d'événements avec la configuration suivante :
   - Cluster Amazon DocumentDB : choisissez le cluster que vous avez créé précédemment.
   - Nom de la base de données : docdbdemo
   - Nom de la collection : products
   - Taille du lot : 1
   - Position de départ : dernière
   - Authentification : BASIC_AUTH
   - Clé Secrets Manager : choisissez le secret de votre cluster Amazon DocumentDB. Cela s'appelle quelque chose `commerds!cluster-12345678-a6f0-52c0-b290-db4aga89274f`.
   - Fenêtre de traitement par lots : 1
   - Configuration complète du document : UpdateLookup

7. Choisissez Ajouter. La création de votre mappage des sources d'événements peut prendre quelques minutes.

Testez votre fonction événementielle

Attendez que le mappage des sources d'événements atteigne l'état Activé. Cela peut prendre plusieurs minutes. Testez ensuite la configuration de bout en bout en insérant, mettant à jour et supprimant des enregistrements de base de données. Avant de commencer :

1. Reconnectez-vous à votre cluster Amazon DocumentDB dans CloudShell votre environnement.
2. Exécutez la commande suivante pour vérifier que vous utilisez bien la `docdbdemo` base de données :

```
use docdbdemo
```

Insérer un enregistrement

Insérez un enregistrement dans la collection `products` de la base de donnée `docdbdemo` :

```
db.products.insertOne({"name":"Pencil", "price": 1.00})
```

Vérifiez que votre fonction a correctement traité cet événement en vérifiant CloudWatch les journaux. Vous devriez voir une entrée de journal comme celle-ci :

Timestamp	Message
2025-05-05T23:55:23.474Z	Operation type: insert
2025-05-05T23:55:23.474Z	db: docdbdemo
2025-05-05T23:55:23.474Z	collection: products
2025-05-05T23:55:23.474Z	Full document: {
2025-05-05T23:55:23.474Z	"_id": {
2025-05-05T23:55:23.474Z	"$oid": "68194fea08d12462ea531d58"
2025-05-05T23:55:23.474Z	},
2025-05-05T23:55:23.474Z	"name": "Pencil",
2025-05-05T23:55:23.474Z	"price": 1
2025-05-05T23:55:23.474Z	}

Mettre à jour un enregistrement

Mettez à jour l'enregistrement que vous venez d'insérer à l'aide de la commande suivante :

```
db.products.updateOne(
    { "name": "Pencil" },
    { $set: { "price": 0.50 }}
)
```

Vérifiez que votre fonction a correctement traité cet événement en vérifiant CloudWatch les journaux. Vous devriez voir une entrée de journal comme celle-ci :

Timestamp	Message
2025-05-05T23:55:27.918Z	Operation type: update
2025-05-05T23:55:27.918Z	db: docdbdemo
2025-05-05T23:55:27.918Z	collection: products
2025-05-05T23:55:27.918Z	Full document: {
2025-05-05T23:55:27.918Z	"_id": {
2025-05-05T23:55:27.918Z	"$oid": "68194fea08d12462ea531d58"
2025-05-05T23:55:27.918Z	},
2025-05-05T23:55:27.918Z	"name": "Pencil",
2025-05-05T23:55:27.918Z	"price": 0.5
2025-05-05T23:55:27.918Z	}

Supprimer un enregistrement

Supprimez l'enregistrement que vous venez de mettre à jour à l'aide de la commande suivante :

```
db.products.deleteOne( { "name": "Pencil" } )
```

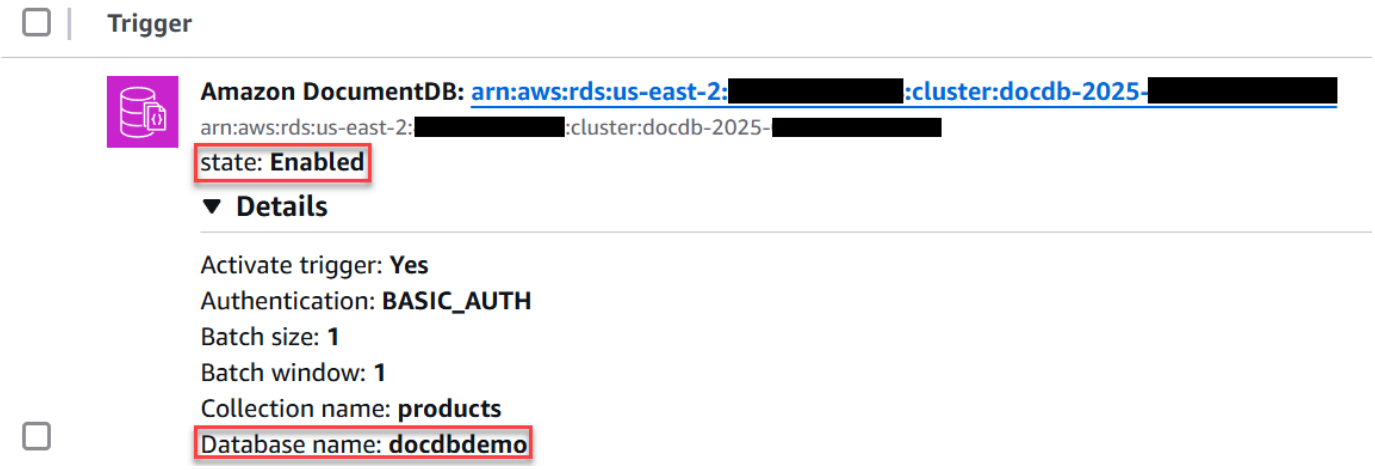
Vérifiez que votre fonction a correctement traité cet événement en vérifiant CloudWatch les journaux. Vous devriez voir une entrée de journal comme celle-ci :

Timestamp	Message
2025-05-05T23:55:32.362Z	Operation type: delete
2025-05-05T23:55:32.362Z	db: docdbdemo
2025-05-05T23:55:32.362Z	collection: products
2025-05-05T23:55:32.362Z	Full document: {}

Résolution des problèmes

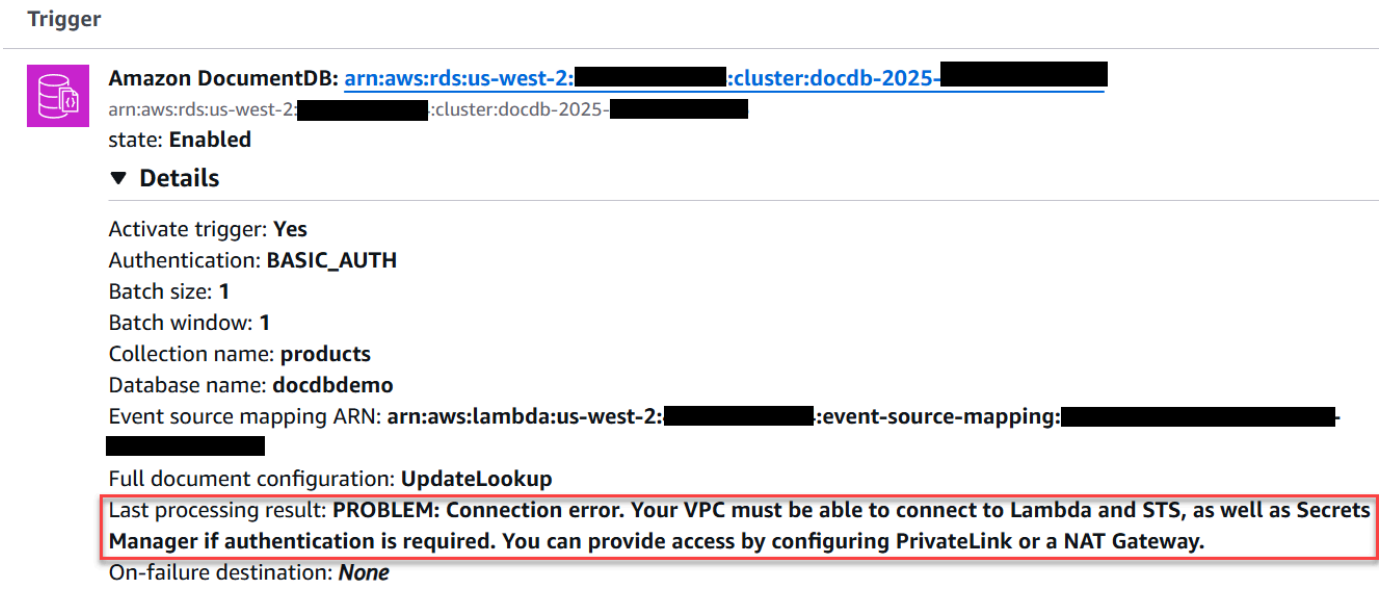
Si aucun événement de base de données n'apparaît dans les CloudWatch journaux de votre fonction, vérifiez les points suivants :

- Assurez-vous que le mappage des sources d'événements Lambda (également appelé déclencheur) est à l'état Activé. La création de mappages des sources d'événements peut prendre plusieurs minutes.
- Si le mappage des sources d'événements est activé mais que les événements de base de données ne s'affichent toujours pas dans CloudWatch :
  - Assurez-vous que le Nom de la base de données dans le mappage des sources d'événements est défini sur `docdbdemo`.



  - Vérifiez si le champ Résultat du dernier traitement du mappage des sources d'événements contient le message « PROBLEM: Connection error. Your VPC must be able to connect to Lambda and STS, as well as Secrets Manager if authentication is required. » Si cette erreur s'affiche, assurez-vous que vous avez créé les points de terminaison de l'interface VPC de

Lambda et Secrets Manager, et que les points de terminaison utilisent le même VPC et les mêmes sous-réseaux que ceux utilisés par votre cluster Amazon DocumentDB.



Nettoyage de vos ressources

Vous pouvez maintenant supprimer les ressources que vous avez créées pour ce didacticiel, sauf si vous souhaitez les conserver. En supprimant des ressources AWS que vous n'utilisez plus, vous évitez les frais superflus pour votre Compte AWS.

Pour supprimer la fonction d'événement Lambda

1. Ouvrez la page Event Functions de la console Lambda.
2. Sélectionnez la fonction d'événement que vous avez créée.
3. Sélectionnez Actions, Supprimer.
4. Saisissez **`confirm`** dans la zone de saisie de texte et choisissez Delete (Supprimer).

Pour supprimer le rôle d'exécution

1. Ouvrez la page Roles (Rôles) de la console IAM.
2. Sélectionnez le rôle d'exécution que vous avez créé.
3. Sélectionnez Supprimer.
4. Saisissez le nom du rôle dans le champ de saisie de texte et choisissez Delete (Supprimer).

Pour supprimer les points de terminaison d'un VPC

1. Ouvrez la console VPC. Dans le menu de gauche, sous Cloud privé virtuel, choisissez Points de terminaison.
2. Sélectionnez les points de terminaison que vous avez créés.
3. Choisissez Actions, Delete VPC endpoints (Supprimer le point de terminaison d'un VPC).
4. Saisissez **`delete`** dans le champ de saisie de texte.
5. Sélectionnez Supprimer.

Pour supprimer le cluster Amazon DocumentDB

1. Ouvrez la console Amazon DocumentDB.
2. Sélectionnez le cluster Amazon DocumentDB que vous avez créé pour ce tutoriel et désactivez la protection contre la suppression.
3. Dans la page principale Clusters, choisissez à nouveau votre cluster Amazon DocumentDB.
4. Sélectionnez Actions, Supprimer.
5. Pour Créer un instantané final du cluster, sélectionnez Non.
6. Saisissez **`delete`** dans le champ de saisie de texte.
7. Sélectionnez Supprimer.

Pour supprimer le secret dans Secrets Manager

1. Ouvrez la console Secrets Manager.
2. Sélectionnez le secret que vous avez créé pour ce tutoriel.
3. Choisissez Actions, Supprimer le secret.
4. Choisissez Schedule deletion (Planifier la suppression).

Utilisation AWS Lambda avec Amazon DynamoDB

> **Note**
>
> Si vous souhaitez envoyer des données à une cible autre qu'une fonction d'événement Lambda ou enrichir les données avant de les envoyer, consultez Amazon EventBridge Pipes.

Vous pouvez utiliser une fonction d' AWS Lambda événement pour traiter les enregistrements d'un flux Amazon DynamoDB. Avec DynamoDB Streams, vous pouvez déclencher une fonction d'événement Lambda pour effectuer des tâches supplémentaires chaque fois qu'une table DynamoDB est mise à jour.

Lorsque vous traitez des flux DynamoDB, vous devez implémenter une logique de réponse partielle de lot afin d'éviter le retraitement d'enregistrements traités avec succès si d'autres enregistrements du lot échouent. L'utilitaire Batch Processor de Powertools for AWS Lambda est disponible en Python TypeScript, .NET et Java et simplifie cette implémentation en gérant automatiquement la logique de réponse partielle par lots, en réduisant le temps de développement et en améliorant la fiabilité.

Rubriques

- Flux d'interrogation et de mise en lots
- Positions de départ des interrogations et des flux
- Lecteurs simultanés d'une partition dans DynamoDB Streams
- Exemple d'évènement
- Traiter les enregistrements DynamoDB avec Lambda
- Configuration d'une réponse par lots partielle avec DynamoDB et Lambda
- Retenir les enregistrements ignorés pour une source d'événement DynamoDB dans Lambda
- Implémentation du traitement des flux DynamoDB avec état dans Lambda
- Paramètres Lambda pour les mappages des sources d'événement Amazon DynamoDB
- Utilisation du filtrage des événements avec une source d'événement DynamoDB
- Tutoriel : Utilisation AWS Lambda avec les flux Amazon DynamoDB

Flux d’interrogation et de mise en lots

Lambda interroge les partitions de votre flux DynamoDB en quête d’enregistrements à une fréquence de base de quatre fois par seconde. Lorsque des enregistrements sont disponibles, Lambda invoque votre fonction et attend le résultat. Si le traitement réussit, Lambda reprend l’interrogation jusqu’à recevoir plus d’enregistrements.

Par défaut, Lambda invoque votre fonction dès que des enregistrements sont disponibles. Si le lot que Lambda lit à partir de la source d’événements ne comprend qu’un seul enregistrement, Lambda envoie un seul registre à la fonction. Pour éviter d’invoquer la fonction avec un petit nombre de registres, vous pouvez indiquer à la source d’événement de les mettre en mémoire tampon pendant 5 minutes en configurant une fenêtre de traitement par lots. Avant d’invoquer la fonction, Lambda continue de lire les registres de la source d’événements jusqu’à ce qu’il ait rassemblé un lot complet, que la fenêtre de traitement par lot expire ou que le lot atteigne la limite de charge utile de 6 Mo. Pour plus d’informations, consultez Comportement de traitement par lots.

> **Warning**
>
> Les mappages des sources d’événements Lambda traitent chaque événement au moins une fois, et le traitement des enregistrements peut être dupliqué. Pour éviter les problèmes potentiels liés à des événements dupliqués, nous vous recommandons vivement de rendre votre code de fonction idempotent. Pour en savoir plus, consultez Comment rendre ma fonction Lambda idempotente dans le Knowledge Center. AWS

Lambda envoi le prochain lot pour traitement sans attendre que les extensions configurées soient terminées. En d’autres termes, vos extensions peuvent continuer à s’exécuter pendant que Lambda traite le prochain lot d’enregistrements. Cela peut causer des problèmes de limitation si vous enfreignez l’un des paramètres ou l’une des limites de simultanéité de votre compte. Pour détecter s’il s’agit d’un problème éventuel, surveillez vos fonctions et vérifiez si vous observez des métriques de simultanéité plus élevées que prévu pour votre mappage des sources d’événements. En raison de la brièveté des intervalles entre les invocations, Lambda peut brièvement signaler une utilisation simultanée supérieure au nombre de partitions. Cela peut être vrai même pour les fonctions d'événement Lambda sans extensions.

Configurez le ParallelizationFactorparamètre pour traiter une partition d'un flux DynamoDB avec plusieurs invocations Lambda simultanément. Vous pouvez spécifier le nombre de lots simultanés que Lambda interroge à partir d'une partition en utilisant un facteur de parallélisation compris

entre 1 (par défaut) et 10. Par exemple, lorsque vous définissez `ParallelizationFactor` la valeur 2, vous pouvez avoir 200 appels Lambda simultanés au maximum pour traiter 100 fragments de flux DynamoDB (bien qu'en pratique, vous puissiez voir des valeurs différentes pour la métrique). `ConcurrentExecutions` Cela permet d'augmenter le débit de traitement quand le volume de données est volatil et que la valeur du paramètre IteratorAge est élevée. Avec`ParallelizationFactor`, Lambda exécute plusieurs lots simultanés par partition et regroupe les enregistrements de chaque partition par clé de partition. Au sein d'une partition, les enregistrements qui partagent une clé de partition sont transférés dans le même lot simultané et sont traités dans l'ordre. Les enregistrements dotés de différentes clés de partition peuvent être traités simultanément. DynamoDB Streams garantit le tri par article (clé de partition et clé de tri). Par conséquent, les enregistrements de flux pour chaque élément apparaissent toujours dans l'ordre dans lequel l'élément a été modifié.

Positions de départ des interrogations et des flux

Sachez que l'interrogation des flux lors des mises à jour et de la création du mappage des sources d'événements est finalement cohérente.

- Lors de la création du mappage des sources d'événements, le démarrage de l'interrogation des événements depuis le flux peut prendre plusieurs minutes.
- Lors des mises à jour du mappage des sources d'événements, l'arrêt et le redémarrage de l'interrogation des événements depuis le flux peuvent prendre plusieurs minutes.

Ce comportement signifie que si vous spécifiez `LATEST` comme position de départ du flux, le mappage des sources d'événements peut manquer des événements lors de la création ou des mises à jour. Pour vous assurer de ne manquer aucun événement, spécifiez la position de départ du flux comme `TRIM_HORIZON`.

Lecteurs simultanés d'une partition dans DynamoDB Streams

Pour les tables à région unique qui ne sont pas des tables globales, vous pouvez concevoir jusqu'à deux fonctions d'événement Lambda pour lire simultanément la même partition DynamoDB Streams. Le dépassement de cette limite peut se traduire par une limitation de la demande. Pour les tables globales, nous vous recommandons de limiter le nombre de fonctions simultanées à une seule pour éviter la limitation des demandes.

Exemple d'évènement

Example

```
{
  "Records": [
    {
      "eventID": "1",
      "eventVersion": "1.0",
      "dynamodb": {
        "Keys": {
          "Id": {
            "N": "101"
          }
        },
        "NewImage": {
          "Message": {
            "S": "New item!"
          },
          "Id": {
            "N": "101"
          }
        },
        "StreamViewType": "NEW_AND_OLD_IMAGES",
        "SequenceNumber": "111",
        "SizeBytes": 26
      },
      "awsRegion": "us-west-2",
      "eventName": "INSERT",
      "eventSourceARN": "arn:aws:dynamodb:us-east-2:123456789012:table/my-table/
stream/2024-06-10T19:26:16.525",
      "eventSource": "aws:dynamodb"
    },
    {
      "eventID": "2",
      "eventVersion": "1.0",
      "dynamodb": {
        "OldImage": {
          "Message": {
            "S": "New item!"
          },
          "Id": {
            "N": "101"
          }
```

```
        },
        "SequenceNumber": "222",
        "Keys": {
          "Id": {
            "N": "101"
          }
        },
        "SizeBytes": 59,
        "NewImage": {
          "Message": {
            "S": "This item has changed"
          },
          "Id": {
            "N": "101"
          }
        },
        "StreamViewType": "NEW_AND_OLD_IMAGES"
      },
      "awsRegion": "us-west-2",
      "eventName": "MODIFY",
      "eventSourceARN": "arn:aws:dynamodb:us-east-2:123456789012:table/my-table/
stream/2024-06-10T19:26:16.525",
      "eventSource": "aws:dynamodb"
    }
  ]}
```

Traiter les enregistrements DynamoDB avec Lambda

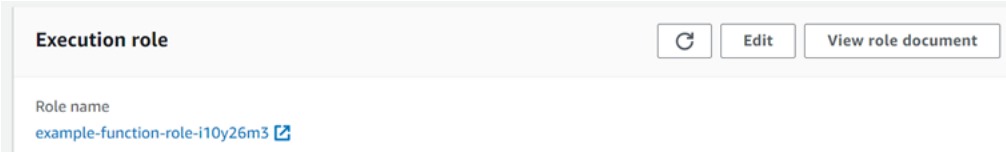
Créez un mappage de source d'événements pour indiquer à Lambda d'envoyer des enregistrements de votre flux vers une fonction d'événement Lambda. Vous pouvez créer plusieurs mappages de sources d'événements pour traiter les mêmes données avec plusieurs fonctions d'événement Lambda, ou pour traiter des éléments provenant de plusieurs flux avec une seule fonction.

Vous pouvez configurer des mappages de sources d’événements pour traiter les enregistrements d’un flux dans un autre Compte AWS. Pour en savoir plus, consultez the section called “Cross-account mappages”.

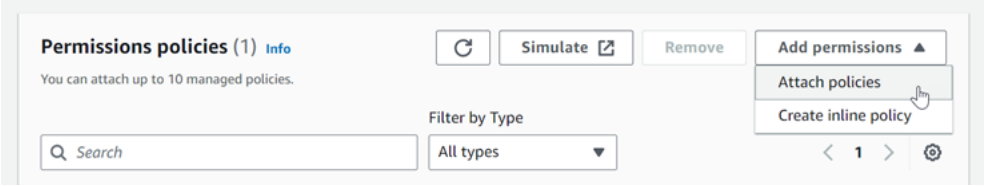
Pour configurer votre fonction de manière à lire depuis DynamoDB Streams, associez la politique AWSLambdaDynamoDBExecutionRole AWS gérée à votre rôle d'exécution, puis créez un déclencheur DynamoDB.

Pour ajouter des autorisations et créer un déclencheur

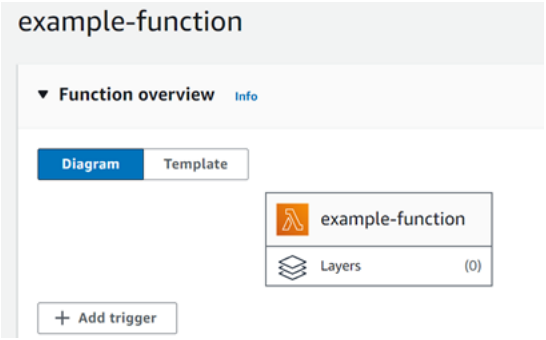
1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez le nom d'une fonction.
3. Choisissez l'onglet Configuration, puis Permissions (Autorisations).
4. Sous Nom du rôle, cliquez sur le lien vers votre rôle d'exécution. Ce lien ouvre le rôle dans la console IAM.



5. Choisissez Ajouter des autorisations, puis Attacher des politiques.



6. Dans le champ de recherche, entrez `AWSLambdaDynamoDBExecutionRole`. Ajoutez cette politique à votre rôle d'exécution. Il s'agit d'une politique AWS gérée qui contient les autorisations dont votre fonction a besoin pour lire le flux DynamoDB. Pour plus d'informations sur cette politique, consultez AWSLambdaDynamoDBExecutionRolela référence des politiques AWS gérées.
7. Revenez à votre fonction dans la console Lambda. Sous Function overview (Vue d'ensemble de la fonction), choisissez Add trigger (Ajouter un déclencheur).



8. Choisissez un type de déclencheur.
9. Configurez les options requises, puis choisissez Add (Ajouter).

Lambda prend en charge les options suivantes pour les sources d'événement DynamoDB :

Options de source d'événement

- DynamoDB table (Table DynamoDB) – Table DynamoDB à partir de laquelle lire les enregistrements.
- Batch size (Taille de lot) – Nombre d'enregistrements par lot à envoyer à la fonction, jusqu'à 10 000. Lambda transmet tous les enregistrements du lot à la fonction en une seule invocation, tant que la taille totale des événements ne dépasse pas la limite de charge utile pour une invocation synchrone (6 Mo).
- Batch window (Fenêtre de traitement par lots) – Intervalle de temps maximum (en secondes) pour collecter des enregistrements avant d'invoquer la fonction.
- Starting position (Position de départ) – Traiter uniquement les nouveaux enregistrements, ou tous enregistrement existants.
  - Latest (Derniers) – Traiter les nouveaux enregistrements ajoutés au flux.
  - Trim horizon (Supprimer l'horizon) – Traiter tous les enregistrements figurant dans le flux.

  Après le traitement de tous les enregistrements existants, la fonction est à jour et continue à traiter les nouveaux enregistrements.
- On-failure destination — Une file d'attente SQS standard ou une rubrique SNS standard pour les enregistrements qui ne peuvent pas être traités. Quand Lambda écarte un lot d'enregistrements qui est trop ancien ou qui a épuisé toutes les tentatives, il envoie les détails du lot à la file d'attente ou à la rubrique.
- Retry attempts (Nouvelles tentatives) – Nombre maximum de nouvelles tentatives que Lambda effectue quand la fonction renvoie une erreur. Cela ne s'applique pas aux erreurs ou limitations de service où le lot n'a pas atteint la fonction.
- Maximum age of record (Âge maximum d'enregistrement) – Âge maximum d'un enregistrement que Lambda envoie à votre fonction.
- Split batch on error (Fractionner le lot en cas d'erreur) – Quand la fonction renvoie une erreur, diviser le lot en deux avant d'effectuer une nouvelle tentative. Le paramètre de taille de lot d'origine reste inchangé.
- Concurrent batches per shard (Lots simultanés par partition) – Traite simultanément plusieurs lots de la même partition.
- Enabled (Activé) – Valeur définie sur VRAI pour activer le mappage de source d'événement. Définissez la valeur sur « false » pour arrêter le traitement des enregistrements. Lambda garde une trace du dernier enregistrement traité et reprend le traitement à ce point lorsque le mappage est réactivé.

> **Note**
>
> Les appels d' GetRecords API invoqués par Lambda dans le cadre des déclencheurs DynamoDB ne vous sont pas facturés.

Pour gérer ultérieurement la configuration de la source d'événement, choisissez le déclencheur dans le concepteur.

Création d'un mappage des sources d'événements entre comptes

Amazon DynamoDB prend désormais en charge les politiques basées sur les ressources. Grâce à cette fonctionnalité, vous pouvez traiter les données d'un flux DynamoDB dans un compte Compte AWS avec une fonction d'événement Lambda dans un autre compte.

Pour créer un mappage de source d'événements pour votre fonction d'événement Lambda à l'aide d'un flux DynamoDB dans un autre Compte AWS, vous devez configurer le flux à l'aide d'une politique basée sur les ressources afin d'autoriser votre fonction d'événement Lambda à lire des enregistrements. Pour savoir comment configurer votre flux pour un accès entre comptes, consultez Partager l'accès avec les fonctions Lambda entre comptes dans le guide du développeur Amazon DynamoDB.

Une fois que vous avez configuré votre flux avec une politique basée sur les ressources qui donne à votre fonction d'événement Lambda les autorisations requises, créez le mappage des sources d'événements avec l'ARN de votre flux entre comptes. Vous pouvez trouver l'ARN du flux sous l'onglet Exportations et flux du tableau dans la console DynamoDB multicomptes.

Lorsque vous utilisez la console Lambda, collez l'ARN du flux directement dans le champ de saisie de la table DynamoDB sur la page de création du mappage des sources d'événements.

Remarque : les Cross-region déclencheurs ne sont pas pris en charge.

Configuration d'une réponse par lots partielle avec DynamoDB et Lambda

Avant de configurer des réponses par lots partielles, vous devez d'abord créer un mappage de source d'événements DynamoDB. Pour obtenir des instructions, consultez the section called "Création d'un mappage".

Lors de l'utilisation et du traitement de données de streaming à partir d'une source d'événement, par défaut, Lambda n'effectue un point de contrôle sur le numéro de séquence le plus élevé d'un lot que lorsque celui-ci est un succès complet. Lambda traite tous les autres résultats

comme un échec complet et recommence à traiter le lot jusqu'à atteindre la limite de nouvelles tentatives. Pour autoriser des succès partiels lors du traitement des lots à partir d'un flux, activez `ReportBatchItemFailures`. Autoriser les réussites partielles peut contribuer à réduire le nombre de tentatives sur un enregistrement, mais cela n'empêche pas totalement la possibilité de nouvelles tentatives dans un enregistrement réussi.

Pour activer `ReportBatchItemFailures`, incluez la valeur enum **`ReportBatchItemFailures`** dans la listeFunctionResponseTypes. Cette liste indique les types de réponse activés pour votre fonction événementielle. Vous pouvez configurer cette liste lorsque vous créez ou mettez à jour un mappage des sources d'événements.

> **Note**
>
> Même lorsque votre code de fonction renvoie des réponses partielles en cas d'échec par lots, ces réponses ne sont pas traitées par Lambda, sauf si la `ReportBatchItemFailures` fonctionnalité est explicitement activée pour le mappage de la source de votre événement.

Syntaxe du rapport

Lors de la configuration des rapports d'échec d'articles de lot, la classe `StreamsEventResponse` est renvoyée avec une liste d'échecs d'articles de lot. Vous pouvez utiliser un objet `StreamsEventResponse` pour renvoyer le numéro de séquence du premier enregistrement ayant échoué dans le lot. Vous pouvez également créer votre classe personnalisée en utilisant la syntaxe de réponse correcte. La structure JSON suivante montre la syntaxe de réponse requise :

```
{
  "batchItemFailures": [
        {
            "itemIdentifier": "<SequenceNumber>"
        }
    ]
}
```

> **Note**
>
> Si le tableau `batchItemFailures` contient plusieurs éléments, Lambda utilise l'enregistrement portant le numéro de séquence le plus bas comme point de contrôle. Lambda réessaie ensuite tous les enregistrements à partir de ce point de contrôle.

Conditions de réussite et d'échec

Lambda traite un lot comme un succès complet si vous renvoyez l'un des éléments suivants :

- Une liste `batchItemFailure` vide
- Une liste `batchItemFailure` nulle
- Une `EventResponse` vide
- Un nu `EventResponse`

Lambda traite un lot comme un échec complet si vous renvoyez l'un des éléments suivants :

- Une chaîne vid `itemIdentifier`
- Un `itemIdentifier` nul
- Un `itemIdentifier` avec un nom de clé incorrect

Lambda effectue des nouvelles tentatives en cas d'échec en fonction de votre stratégie de nouvelle tentative.

Diviser un lot

Si votre invocation échoue et que `BisectBatchOnFunctionError` est activé, le lot est divisé en deux quel que soit votre paramètre `ReportBatchItemFailures`.

Quand une réponse de succès partiel de lot est reçue et que les paramètres `BisectBatchOnFunctionError` et `ReportBatchItemFailures` sont activés, le lot est divisé au numéro de séquence renvoyé, et Lambda n'effectue de nouvelle tentative que sur les enregistrements restants.

Pour simplifier la mise en œuvre de la logique de réponse partielle par lots, pensez à utiliser l'utilitaire Batch Processor de Powertools for AWS Lambda, qui gère automatiquement ces complexités pour vous.

Voici quelques exemples de codes de fonctions qui renvoient la liste des identifiants des messages ayant échoué dans le lot :

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signalement des échecs d'articles par lots DynamoDB avec Lambda à l'aide de .NET.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
using System.Text.Json;
using System.Text;
using Amazon.Lambda.Core;
using Amazon.Lambda.DynamoDBEvents;

// Assembly attribute to enable the Lambda function's JSON input to be converted
 into a .NET class.
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSeri

namespace AWSLambda_DDB;

public class Function
{
    public StreamsEventResponse FunctionHandler(DynamoDBEvent dynamoEvent,
 ILambdaContext context)

    {
        context.Logger.LogInformation($"Beginning to process
 {dynamoEvent.Records.Count} records...");
        List<StreamsEventResponse.BatchItemFailure> batchItemFailures = new
 List<StreamsEventResponse.BatchItemFailure>();
        StreamsEventResponse streamsEventResponse = new StreamsEventResponse();

        foreach (var record in dynamoEvent.Records)
        {
            try
            {
                var sequenceNumber = record.Dynamodb.SequenceNumber;
```

```
                context.Logger.LogInformation(sequenceNumber);
            }
            catch (Exception ex)
            {
                context.Logger.LogError(ex.Message);
                batchItemFailures.Add(new StreamsEventResponse.BatchItemFailure()
 { ItemIdentifier = record.Dynamodb.SequenceNumber });
            }
        }

        if (batchItemFailures.Count > 0)
        {
            streamsEventResponse.BatchItemFailures = batchItemFailures;
        }

        context.Logger.LogInformation("Stream processing complete.");
        return streamsEventResponse;
    }
}
```

Go

Kit SDK pour Go V2

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signalement des échecs d'articles par lots DynamoDB avec Lambda à l'aide de Go.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package main

import (
 "context"
 "github.com/aws/aws-lambda-go/events"
 "github.com/aws/aws-lambda-go/lambda"
)
```

```
type BatchItemFailure struct {
 ItemIdentifier string `json:"ItemIdentifier"`
}

type BatchResult struct {
 BatchItemFailures []BatchItemFailure `json:"BatchItemFailures"`
}

func HandleRequest(ctx context.Context, event events.DynamoDBEvent)
 (*BatchResult, error) {
 var batchItemFailures []BatchItemFailure
 curRecordSequenceNumber := ""

 for _, record := range event.Records {
  // Process your record
  curRecordSequenceNumber = record.Change.SequenceNumber
 }

 if curRecordSequenceNumber != "" {
  batchItemFailures = append(batchItemFailures, BatchItemFailure{ItemIdentifier:
 curRecordSequenceNumber})
 }

 batchResult := BatchResult{
  BatchItemFailures: batchItemFailures,
 }

 return &batchResult, nil
}

func main() {
 lambda.Start(HandleRequest)
}
```

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signalement des échecs d'articles par lots DynamoDB avec Lambda à l'aide de Java.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.DynamodbEvent;
import com.amazonaws.services.lambda.runtime.events.StreamsEventResponse;
import com.amazonaws.services.lambda.runtime.events.models.dynamodb.StreamRecord;

import java.util.ArrayList;
import java.util.List;

public class ProcessDynamodbRecords implements RequestHandler<DynamodbEvent,
 StreamsEventResponse> {

    @Override
    public StreamsEventResponse handleRequest(DynamodbEvent input, Context
 context) {

        List<StreamsEventResponse.BatchItemFailure> batchItemFailures = new
 ArrayList<>();
        String curRecordSequenceNumber = "";

        for (DynamodbEvent.DynamodbStreamRecord dynamodbStreamRecord :
 input.getRecords()) {
          try {
                //Process your record
                StreamRecord dynamodbRecord = dynamodbStreamRecord.getDynamodb();
                curRecordSequenceNumber = dynamodbRecord.getSequenceNumber();

            } catch (Exception e) {
```

```
                /* Since we are working with streams, we can return the failed
 item immediately.
                   Lambda will immediately begin to retry processing from this
 failed item onwards. */
                batchItemFailures.add(new
 StreamsEventResponse.BatchItemFailure(curRecordSequenceNumber));
                return new StreamsEventResponse(batchItemFailures);
            }
        }

       return new StreamsEventResponse();
    }
}
```

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signaler les défaillances d'éléments de lot DynamoDB avec Lambda à l'aide de. JavaScript

```
export const handler = async (event) => {
  const records = event.Records;
  let curRecordSequenceNumber = "";

  for (const record of records) {
    try {
      // Process your record
      curRecordSequenceNumber = record.dynamodb.SequenceNumber;
    } catch (e) {
      // Return failed record's sequence number
      return { batchItemFailures: [{ itemIdentifier:
 curRecordSequenceNumber }] };
    }
  }
```

```
  return { batchItemFailures: [] };
};
```

Signaler les défaillances d'éléments de lot DynamoDB avec Lambda à l'aide de. TypeScript

```
import {
  DynamoDBBatchResponse,
  DynamoDBBatchItemFailure,
  DynamoDBStreamEvent,
} from "aws-lambda";

export const handler = async (
  event: DynamoDBStreamEvent
): Promise<DynamoDBBatchResponse> => {
  const batchItemFailures: DynamoDBBatchItemFailure[] = [];
  let curRecordSequenceNumber;

  for (const record of event.Records) {
    curRecordSequenceNumber = record.dynamodb?.SequenceNumber;

    if (curRecordSequenceNumber) {
      batchItemFailures.push({
        itemIdentifier: curRecordSequenceNumber,
      });
    }
  }

  return { batchItemFailures: batchItemFailures };
};
```

PHP

Kit SDK pour PHP

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signalement des échecs d'articles par lots DynamoDB avec Lambda à l'aide de PHP.

```
<?php

# using bref/bref and bref/logger for simplicity

use Bref\Context\Context;
use Bref\Event\DynamoDb\DynamoDbEvent;
use Bref\Event\Handler as StdHandler;
use Bref\Logger\StderrLogger;

require __DIR__ . '/vendor/autoload.php';

class Handler implements StdHandler
{
    private StderrLogger $logger;
    public function __construct(StderrLogger $logger)
    {
        $this->logger = $logger;
    }

    /**
     * @throws JsonException
     * @throws \Bref\Event\InvalidLambdaEvent
     */
    public function handle(mixed $event, Context $context): array
    {
        $dynamoDbEvent = new DynamoDbEvent($event);
        $this->logger->info("Processing records");

        $records = $dynamoDbEvent->getRecords();
        $failedRecords = [];
        foreach ($records as $record) {
            try {
                $data = $record->getData();
                $this->logger->info(json_encode($data));
                // TODO: Do interesting work based on the new data
            } catch (Exception $e) {
                $this->logger->error($e->getMessage());
                // failed processing the record
                $failedRecords[] = $record->getSequenceNumber();
            }
        }
        $totalRecords = count($records);
```

```
        $this->logger->info("Successfully processed $totalRecords records");

        // change format for the response
        $failures = array_map(
            fn(string $sequenceNumber) => ['itemIdentifier' => $sequenceNumber],
            $failedRecords
        );

        return [
            'batchItemFailures' => $failures
        ];
    }
}

$logger = new StderrLogger();
return new Handler($logger);
```

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signalement des échecs d'articles par lots DynamoDB avec Lambda à l'aide de Python.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
def handler(event, context):
    records = event.get("Records")
    curRecordSequenceNumber = ""

    for record in records:
        try:
            # Process your record
            curRecordSequenceNumber = record["dynamodb"]["SequenceNumber"]
        except Exception as e:
            # Return failed record's sequence number
```

```
            return {"batchItemFailures":[{"itemIdentifier":
 curRecordSequenceNumber}]}

    return {"batchItemFailures":[]}
```

Ruby

Kit SDK pour Ruby

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signalement des échecs d'articles par lots DynamoDB avec Lambda à l'aide de Ruby.

```
def lambda_handler(event:, context:)
    records = event["Records"]
    cur_record_sequence_number = ""

    records.each do |record|
      begin
        # Process your record
        cur_record_sequence_number = record["dynamodb"]["SequenceNumber"]
      rescue StandardError => e
        # Return failed record's sequence number
        return {"batchItemFailures" => [{"itemIdentifier" =>
 cur_record_sequence_number}]}
      end
    end

    {"batchItemFailures" => []}
  end
```

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signalement des échecs d'articles par lots DynamoDB avec Lambda à l'aide de Rust.

```
use aws_lambda_events::{
    event::dynamodb::{Event, EventRecord, StreamRecord},
    streams::{DynamoDbBatchItemFailure, DynamoDbEventResponse},
};
use lambda_runtime::{run, service_fn, Error, LambdaEvent};

/// Process the stream record
fn process_record(record: &EventRecord) -> Result<(), Error> {
    let stream_record: &StreamRecord = &record.change;

    // process your stream record here...
    tracing::info!("Data: {:?}", stream_record);

    Ok(())
}

/// Main Lambda handler here...
async fn function_handler(event: LambdaEvent<Event>) ->
 Result<DynamoDbEventResponse, Error> {
    let mut response = DynamoDbEventResponse {
        batch_item_failures: vec![],
    };

    let records = &event.payload.records;

    if records.is_empty() {
        tracing::info!("No records found. Exiting.");
        return Ok(response);
    }

    for record in records {
```

```
        tracing::info!("EventId: {}", record.event_id);

        // Couldn't find a sequence number
        if record.change.sequence_number.is_none() {
            response.batch_item_failures.push(DynamoDbBatchItemFailure {
                item_identifier: Some("".to_string()),
            });
            return Ok(response);
        }

        // Process your record here...
        if process_record(record).is_err() {
            response.batch_item_failures.push(DynamoDbBatchItemFailure {
                item_identifier: record.change.sequence_number.clone(),
            });
            /* Since we are working with streams, we can return the failed item
 immediately.
            Lambda will immediately begin to retry processing from this failed
 item onwards. */
            return Ok(response);
        }
    }

    tracing::info!("Successfully processed {} record(s)", records.len());

    Ok(response)
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    tracing_subscriber::fmt()
        .with_max_level(tracing::Level::INFO)
        // disable printing the name of the module in every log line.
        .with_target(false)
        // disabling time is handy because CloudWatch will add the ingestion
 time.
        .without_time()
        .init();

    run(service_fn(function_handler)).await
}
```

Utilisation de Powertools pour AWS Lambda processeur par lots

L'utilitaire de traitement par lots de Powertools for gère AWS Lambda automatiquement la logique de réponse partielle par lots, réduisant ainsi la complexité de la mise en œuvre du signalement des défaillances par lots. Voici des exemples d'utilisation de l'utilitaire de traitement par lots :

Python

> **Note**
>
> Pour des exemples complets et des instructions de configuration, consultez la documentation de l'utilitaire de traitement par lots.

Traitement des enregistrements AWS Lambda de flux DynamoDB à l'aide d'un processeur par lots.

```
import json
from aws_lambda_powertools import Logger
from aws_lambda_powertools.utilities.batch import BatchProcessor, EventType,
 process_partial_response
from aws_lambda_powertools.utilities.data_classes import DynamoDBStreamEvent
from aws_lambda_powertools.utilities.typing import LambdaContext

processor = BatchProcessor(event_type=EventType.DynamoDBStreams)
logger = Logger()

def record_handler(record):
    logger.info(record)
    # Your business logic here
    # Raise an exception to mark this record as failed

def lambda_handler(event, context: LambdaContext):
    return process_partial_response(
        event=event,
        record_handler=record_handler,
        processor=processor,
        context=context
    )
```

TypeScript

> **Note**
>
> Pour des exemples complets et des instructions de configuration, consultez la documentation de l'utilitaire de traitement par lots.

Traitement des enregistrements AWS Lambda de flux DynamoDB à l'aide d'un processeur par lots.

```
import { BatchProcessor, EventType, processPartialResponse } from '@aws-lambda-
powertools/batch';
import { Logger } from '@aws-lambda-powertools/logger';
import type { DynamoDBStreamEvent, Context } from 'aws-lambda';

const processor = new BatchProcessor(EventType.DynamoDBStreams);
const logger = new Logger();

const recordHandler = async (record: any): Promise<void> => {
    logger.info('Processing record', { record });
    // Your business logic here
    // Throw an error to mark this record as failed
};

export const handler = async (event: DynamoDBStreamEvent, context: Context) => {
    return processPartialResponse(event, recordHandler, processor, {
        context,
    });
};
```

Java

> **Note**
>
> Pour des exemples complets et des instructions de configuration, consultez la documentation de l'utilitaire de traitement par lots.

Traitement des enregistrements AWS Lambda de flux DynamoDB à l'aide d'un processeur par lots.

```
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.DynamodbEvent;
import com.amazonaws.services.lambda.runtime.events.StreamsEventResponse;
import software.amazon.lambda.powertools.batch.BatchMessageHandlerBuilder;
import software.amazon.lambda.powertools.batch.handler.BatchMessageHandler;

public class DynamoDBStreamBatchHandler implements RequestHandler<DynamodbEvent,
 StreamsEventResponse> {

    private final BatchMessageHandler<DynamodbEvent, StreamsEventResponse> handler;

    public DynamoDBStreamBatchHandler() {
        handler = new BatchMessageHandlerBuilder()
                .withDynamoDbBatchHandler()
                .buildWithRawMessageHandler(this::processMessage);
    }

    @Override
    public StreamsEventResponse handleRequest(DynamodbEvent ddbEvent, Context
 context) {
        return handler.processBatch(ddbEvent, context);
    }

    private void processMessage(DynamodbEvent.DynamodbStreamRecord
 dynamodbStreamRecord, Context context) {
        // Process the change record
    }
}
```

.NET

> **Note**
>
> Pour des exemples complets et des instructions de configuration, consultez la documentation de l'utilitaire de traitement par lots.

Traitement des enregistrements AWS Lambda de flux DynamoDB à l'aide d'un processeur par lots.

```
using System;
```

```
using System.Threading;
using System.Threading.Tasks;
using Amazon.Lambda.Core;
using Amazon.Lambda.DynamoDBEvents;
using Amazon.Lambda.Serialization.SystemTextJson;
using AWS.Lambda.Powertools.BatchProcessing;

[assembly: LambdaSerializer(typeof(DefaultLambdaJsonSerializer))]

namespace HelloWorld;

public class Customer
{
    public string? CustomerId { get; set; }
    public string? Name { get; set; }
    public string? Email { get; set; }
    public DateTime CreatedAt { get; set; }
}

internal class TypedDynamoDbRecordHandler : ITypedRecordHandler<Customer>
{
    public async Task<RecordHandlerResult> HandleAsync(Customer customer,
 CancellationToken cancellationToken)
    {
        if (string.IsNullOrEmpty(customer.Email))
        {
            throw new ArgumentException("Customer email is required");
        }

        return await Task.FromResult(RecordHandlerResult.None);
    }
}

public class Function
{
    [BatchProcessor(TypedRecordHandler = typeof(TypedDynamoDbRecordHandler))]
    public BatchItemFailuresResponse HandlerUsingTypedAttribute(DynamoDBEvent _)
    {
        return TypedDynamoDbStreamBatchProcessor.Result.BatchItemFailuresResponse;
    }
}
```

Retenir les enregistrements ignorés pour une source d'événement DynamoDB dans Lambda

La gestion des erreurs pour les mappages de sources d'événements DynamoDB dépend du fait que l'erreur se produit avant que la fonction d'événement ne soit invoquée ou pendant l'invocation de la fonction :

- Avant l'appel : si un mappage de source d'événement Lambda ne parvient pas à appeler la fonction en raison d'un ralentissement ou d'autres problèmes, il réessaie jusqu'à ce que les enregistrements expirent ou dépassent l'âge maximum configuré sur le mappage de source d'événement (). MaximumRecordAgeInSeconds
- Pendant l'appel : si la fonction est invoquée mais renvoie une erreur, Lambda réessaie jusqu'à ce que les enregistrements expirent, dépassent l'âge maximum MaximumRecordAgeInSeconds() ou atteignent le quota de nouvelles tentatives configuré (). MaximumRetryAttempts Pour les erreurs de fonctionnement, vous pouvez également configurer BisectBatchOnFunctionError, ce qui divise un lot défaillant en deux lots plus petits, isolant ainsi les mauvais enregistrements et évitant les délais d'attente. Le fractionnement des lots ne consomme pas le quota de nouvelles tentatives.

Si les mesures de gestion des erreurs échouent, Lambda ignore les enregistrements et poursuit le traitement des lots du flux. Avec les paramètres par défaut, cela signifie qu'un enregistrement défectueux peut bloquer le traitement sur la partition affectée pendant jusqu'à une journée. Pour éviter cela, configurez le mappage de source d'événement de votre fonction avec un nombre raisonnable de nouvelles tentatives et un âge maximum d'enregistrement correspondant à votre cas d'utilisation.

Configuration des destinations pour les invocations ayant échoué

Pour conserver les enregistrements des appels de mappage des sources d'événements ayant échoué, ajoutez une destination au mappage des sources d'événements de votre fonction d'événement. Chaque enregistrement envoyé à la destination est un document JSON contenant les métadonnées sur l'invocation ayant échoué. Pour les destinations Amazon S3, Lambda envoie également l'intégralité de l'enregistrement d'invocation avec les métadonnées. Vous pouvez configurer n'importe quelle rubrique Amazon SNS, n'importe quelle file d'attente Amazon SQS, n'importe quel compartiment Amazon S3 ou Kafka comme destination.

Avec les destinations Amazon S3, vous pouvez utiliser la fonctionnalité Notifications d'événements Amazon S3 pour recevoir des notifications lorsque des objets sont chargés dans votre compartiment S3 de destination. Vous pouvez également configurer les notifications d'événements S3 pour appeler

une autre fonction d'événement Lambda afin d'effectuer un traitement automatique des lots ayant échoué.

Votre rôle d'exécution doit disposer d'autorisations pour la destination :

- Pour une destination SQS : sqs : SendMessage
- Pour une destination SNS : SNS:Publish
- Pour une destination S3 : s3 : PutObject et s3 : ListBucket
- Pour une destination Kafka : kafka-cluster : WriteData

Vous pouvez configurer un sujet Kafka comme destination en cas d'échec pour vos mappages de sources d'événements Kafka. Lorsque Lambda ne parvient pas à traiter les enregistrements après avoir épuisé toutes les tentatives ou lorsque les enregistrements dépassent l'âge maximum, Lambda envoie les enregistrements ayant échoué à la rubrique Kafka spécifiée pour un traitement ultérieur. Reportez-vous à the section called “Destination de Kafka en cas d'échec”.

Si vous avez activé le chiffrement avec votre propre clé KMS pour une destination S3, le rôle d'exécution de votre fonction doit également être autorisé à appeler kms : GenerateDataKey. Si la clé KMS et la destination du compartiment S3 se trouvent dans un compte différent de celui de votre fonction d'événement Lambda et de votre rôle d'exécution, configurez la clé KMS de manière à ce que le rôle d'exécution autorise les km :. GenerateDataKey

Pour configurer une destination en cas de panne à l'aide de la console, procédez comme suit :

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez une fonction.
3. Sous Function overview (Vue d'ensemble de la fonction), choisissez Add destination (Ajouter une destination).
4. Pour Source, choisissez Invocation du mappage des sources d'événements.
5. Pour le mappage des sources d'événements, choisissez une source d'événements configurée pour cette fonction.
6. Pour Condition, sélectionnez En cas d'échec. Pour les invocations de mappage des sources d'événements, il s'agit de la seule condition acceptée.
7. Pour Type de destination, choisissez le type de destination auquel Lambda envoie les enregistrements d'invocation.
8. Pour Destination, choisissez une ressource.

9. Cliquez sur Enregistrer.

Vous pouvez également configurer une destination en cas de panne à l'aide de AWS Command Line Interface (AWS CLI). Par exemple, la commande create-event-source-mapping suivante ajoute un mappage des sources d'événements avec une destination SQS en cas d'échec à `MyFunction` :

```
aws lambda create-event-source-mapping \
--function-name "MyFunction" \
--event-source-arn arn:aws:dynamodb:us-east-2:123456789012:table/my-table/
stream/2024-06-10T19:26:16.525 \
--destination-config '{"OnFailure": {"Destination": "arn:aws:sqs:us-
east-1:123456789012:dest-queue"}}'
```

La commande update-event-source-mapping suivante met à jour un mappage des sources d'événements pour envoyer les enregistrements d'invocation ayant échoué à une destination SNS après deux nouvelles tentatives, ou si les enregistrements datent de plus d'une heure.

```
aws lambda update-event-source-mapping \
--uuid f89f8514-cdd9-4602-9e1f-01a5b77d449b \
--maximum-retry-attempts 2 \
--maximum-record-age-in-seconds 3600 \
--destination-config '{"OnFailure": {"Destination": "arn:aws:sns:us-
east-1:123456789012:dest-topic"}}'
```

Les paramètres mis à jour sont appliqués de façon asynchrone et ne sont pas reflétés dans la sortie tant que le processus n'est pas terminé. Utilisez la commande get-event-source-mapping pour afficher l'état actuel.

Pour supprimer une destination, entrez une chaîne vide comme argument du paramètre `destination-config` :

```
aws lambda update-event-source-mapping \
--uuid f89f8514-cdd9-4602-9e1f-01a5b77d449b \
--destination-config '{"OnFailure": {"Destination": ""}}'
```

Pratiques exemplaires en matière de sécurité pour les destinations Amazon S3

La suppression d'un compartiment S3 configuré comme destination sans supprimer la destination de la configuration de votre fonction peut engendrer un risque de sécurité. Si un autre utilisateur connaît le nom de votre compartiment de destination, il peut recréer le compartiment dans son Compte AWS.

Les enregistrements des invocations ayant échoué seront envoyés dans son compartiment, exposant potentiellement les données de votre fonction.

> **Warning**
>
> Pour vous assurer que les enregistrements d'invocation de votre fonction d'événement ne peuvent pas être envoyés vers un compartiment S3 d'un autre Compte AWS, ajoutez une condition au rôle d'exécution de votre fonction qui limite `s3:PutObject` les autorisations aux compartiments de votre compte.

L'exemple suivant présente une politique IAM qui limite les autorisations `s3:PutObject` de votre fonction aux seuls compartiments de votre compte. Cette politique donne également à Lambda l'autorisation `s3:ListBucket` dont il a besoin pour utiliser un compartiment S3 comme destination.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3BucketResourceAccountWrite",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::*/*",
                "arn:aws:s3:::*"
            ],
            "Condition": {
                "StringEquals": {
                    "s3:ResourceAccount": "111122223333"
                }
            }
        }
    ]
}
```

Pour ajouter une politique d'autorisations au rôle d'exécution de votre fonction à l'aide du Console de gestion AWS ou AWS CLI, reportez-vous aux instructions des procédures suivantes :

Console

Pour ajouter une politique d'autorisations au rôle d'exécution d'une fonction (console)

1. Ouvrez la page Event Functions de la console Lambda.
2. Sélectionnez la fonction d'événement Lambda dont vous souhaitez modifier le rôle d'exécution.
3. Sous l'onglet Configuration, sélectionnez Autorisations.
4. Sous l'onglet Rôle d'exécution, sélectionnez le Nom du rôle de votre fonction pour ouvrir la page de console IAM du rôle.
5. Ajoutez une politique d'autorisations de au rôle en procédant comme suit :
   a. Dans le volet Politiques d'autorisations, choisissez Ajouter des autorisations, puis Créer une politique en ligne.
   b. Dans l'Éditeur de politique, sélectionnez JSON.
   c. Collez la politique que vous souhaitez ajouter dans l'éditeur (en remplacement du JSON existant), puis choisissez Suivant.
   d. Sous Détails de la politique, saisissez un Nom de la politique.
   e. Choisissez Create Policy (Créer une politique).

AWS CLI

Pour ajouter une politique d'autorisation au rôle d'exécution (CLI) d'une fonction d'événement

1. Créez un document de politique JSON avec les autorisations requises et enregistrez-le dans un répertoire local.
2. Utilisez la commande `put-role-policy` de la CLI IAM pour ajouter des autorisations au rôle d'exécution de votre fonction. Exécutez la commande suivante depuis le répertoire dans lequel vous avez enregistré votre document de politique JSON et remplacez le nom du rôle, le nom de la politique et le document de politique par vos propres valeurs.

```
aws iam put-role-policy \
--role-name my_lambda_role \
--policy-name LambdaS3DestinationPolicy \
--policy-document file://my_policy.json
```

Exemple d'enregistrement d'invocation Amazon SNS et Amazon SQS

L'exemple suivant illustre un enregistrement d'invocation que Lambda envoie à une destination SQS ou SNS pour un flux DynamoDB.

```
{
    "requestContext": {
        "requestId": "316aa6d0-8154-xmpl-9af7-85d5f4a6bc81",
        "functionArn": "arn:aws:lambda:us-east-2:123456789012:function:myfunction",
        "condition": "RetryAttemptsExhausted",
        "approximateInvokeCount": 1
    },
    "responseContext": {
        "statusCode": 200,
        "executedVersion": "$LATEST",
        "functionError": "Unhandled"
    },
    "version": "1.0",
    "timestamp": "2019-11-14T00:13:49.717Z",
    "DDBStreamBatchInfo": {
        "shardId": "shardId-00000001573689847184-864758bb",
        "startSequenceNumber": "800000000003126276362",
        "endSequenceNumber": "800000000003126276362",
        "approximateArrivalOfFirstRecord": "2019-11-14T00:13:19Z",
        "approximateArrivalOfLastRecord": "2019-11-14T00:13:19Z",
        "batchSize": 1,
        "streamArn": "arn:aws:dynamodb:us-east-2:123456789012:table/mytable/
stream/2019-11-14T00:04:06.388"
    }
}
```

Vous pouvez utiliser ces informations pour récupérer les enregistrements concernés à partir du flux à des fins de résolution de problèmes. Les enregistrements réels n'étant pas inclus, vous devez les récupérer du flux avant qu'ils expirent et soient perdus.

Exemple d'enregistrement d'invocation Amazon S3

L'exemple suivant illustre un enregistrement d'invocation que Lambda envoie à un compartiment S3 pour un flux DynamoDB. Outre tous les champs de l'exemple précédent pour les destinations SQS et SNS, le champ `payload` contient l'enregistrement d'invocation d'origine sous forme de chaîne JSON échappée.

```
{
    "requestContext": {
        "requestId": "316aa6d0-8154-xmpl-9af7-85d5f4a6bc81",
        "functionArn": "arn:aws:lambda:us-east-2:123456789012:function:myfunction",
        "condition": "RetryAttemptsExhausted",
        "approximateInvokeCount": 1
    },
    "responseContext": {
        "statusCode": 200,
        "executedVersion": "$LATEST",
        "functionError": "Unhandled"
    },
    "version": "1.0",
    "timestamp": "2019-11-14T00:13:49.717Z",
    "DDBStreamBatchInfo": {
        "shardId": "shardId-00000001573689847184-864758bb",
        "startSequenceNumber": "800000000003126276362",
        "endSequenceNumber": "800000000003126276362",
        "approximateArrivalOfFirstRecord": "2019-11-14T00:13:19Z",
        "approximateArrivalOfLastRecord": "2019-11-14T00:13:19Z",
        "batchSize": 1,
        "streamArn": "arn:aws:dynamodb:us-east-2:123456789012:table/mytable/
stream/2019-11-14T00:04:06.388"
    },
    "payload": "<Whole Event>" // Only available in S3
}
```

L’objet S3 contenant l’enregistrement d’invocation utilise la convention de dénomination suivante :

```
aws/lambda/<ESM-UUID>/<shardID>/YYYY/MM/DD/YYYY-MM-DDTHH.MM.SS-<Random UUID>
```

Implémentation du traitement des flux DynamoDB avec état dans Lambda

Les fonctions d'événement Lambda peuvent exécuter des applications de traitement de flux continu. Un flux représente des données illimitées qui circulent en continu dans votre application. Pour analyser les informations provenant de cette entrée de mise à jour continue, vous pouvez lier les enregistrements inclus à l’aide d’une fenêtre de temps définie.

Les fenêtres bascules sont des fenêtres temporelles distinctes qui s’ouvrent et se ferment à intervalles réguliers. Par défaut, les invocations Lambda sont sans état : vous ne pouvez pas les

utiliser pour traiter des données sur plusieurs invocations continues sans base de données externe. Cependant, avec les fenêtres bascules, vous pouvez maintenir votre état au long des invocations.

Cet état contient le résultat global des messages précédemment traités pour la fenêtre actuelle. Votre état peut atteindre un maximum de 1 Mo pour chaque partition. S'il dépasse cette taille, Lambda met fin précocement à la fenêtre de traitement.

Chaque enregistrement d'un flux appartient à une fenêtre spécifique. Lambda traite chaque enregistrement au moins une fois, mais ne garantit pas que chaque enregistrement ne soit traité qu'une seule fois. Dans de rares cas, tels que pour la gestion des erreurs, certains enregistrements peuvent être sujet à de multiples traitements. Les dossiers sont toujours traités dans l'ordre dès la première fois. Si les enregistrements sont traités plusieurs fois, ils peuvent être traités dans le désordre.

Regroupement et traitement

Votre fonction gérée par l'utilisateur est invoquée tant pour l'agrégation que pour le traitement des résultats finaux de celle-ci. Lambda regroupe tous les enregistrements reçus dans la fenêtre. Vous pouvez recevoir ces enregistrements en plusieurs lots, chacun sous forme d'invocation séparée. Chaque invocation reçoit un état.

Ainsi, lorsque vous utilisez des fenêtres coulissantes, la réponse de votre fonction d'événement Lambda doit contenir `state` une propriété. Si la réponse ne contient pas de propriété `state`, Lambda considère qu'il s'agit d'une invocation ayant échoué. Pour satisfaire à cette condition, votre fonction peut renvoyer un objet `TimeWindowEventResponse` ayant la forme JSON suivante :

Example **`TimeWindowEventResponse`** values

```
{
    "state": {
        "1": 282,
        "2": 715
    },
    "batchItemFailures": []
}
```

> **Note**
>
> Pour les fonctions Java, nous vous recommandons d'utiliser `Map<String, String>` pour représenter l'état.

À la fin de la fenêtre, l'indicateur `isFinalInvokeForWindow` est configuré `true` pour indiquer qu'il s'agit de l'état final et qu'il est prêt à être traité. Après le traitement, la fenêtre et votre invocation final se terminent, puis l'état est supprimé.

À la fin de votre fenêtre, Lambda applique un traitement final pour les actions sur les résultats de l'agrégation. Votre traitement final est invoqué de manière synchrone. Une fois l'invocation réussie, votre fonction contrôle le numéro de séquence et le traitement du flux continue. Si l'invocation échoue, votre fonction d'événement Lambda suspend le traitement ultérieur jusqu'à ce que l'appel aboutisse.

Example DynamodbTimeWindowEvent


```
{
   "Records":[
      {
         "eventID":"1",
         "eventName":"INSERT",
         "eventVersion":"1.0",
         "eventSource":"aws:dynamodb",
         "awsRegion":"us-east-1",
         "dynamodb":{
            "Keys":{
               "Id":{
                  "N":"101"
               }
            },
            "NewImage":{
               "Message":{
                  "S":"New item!"
               },
               "Id":{
                  "N":"101"
               }
            },
            "SequenceNumber":"111",
            "SizeBytes":26,
            "StreamViewType":"NEW_AND_OLD_IMAGES"
         },
         "eventSourceARN":"stream-ARN"
      },
      {
         "eventID":"2",
```

```
         "eventName":"MODIFY",
         "eventVersion":"1.0",
         "eventSource":"aws:dynamodb",
         "awsRegion":"us-east-1",
         "dynamodb":{
            "Keys":{
               "Id":{
                  "N":"101"
               }
            },
            "NewImage":{
               "Message":{
                  "S":"This item has changed"
               },
               "Id":{
                  "N":"101"
               }
            },
            "OldImage":{
               "Message":{
                  "S":"New item!"
               },
               "Id":{
                  "N":"101"
               }
            },
            "SequenceNumber":"222",
            "SizeBytes":59,
            "StreamViewType":"NEW_AND_OLD_IMAGES"
         },
         "eventSourceARN":"stream-ARN"
      },
      {
         "eventID":"3",
         "eventName":"REMOVE",
         "eventVersion":"1.0",
         "eventSource":"aws:dynamodb",
         "awsRegion":"us-east-1",
         "dynamodb":{
            "Keys":{
               "Id":{
                  "N":"101"
               }
            },
```

```
            "OldImage":{
               "Message":{
                  "S":"This item has changed"
               },
               "Id":{
                  "N":"101"
               }
            },
            "SequenceNumber":"333",
            "SizeBytes":38,
            "StreamViewType":"NEW_AND_OLD_IMAGES"
         },
         "eventSourceARN":"stream-ARN"
      }
   ],
    "window": {
        "start": "2020-07-30T17:00:00Z",
        "end": "2020-07-30T17:05:00Z"
    },
    "state": {
        "1": "state1"
    },
    "shardId": "shard123456789",
    "eventSourceARN": "stream-ARN",
    "isFinalInvokeForWindow": false,
    "isWindowTerminatedEarly": false
}
```

Configuration

Vous pouvez configurer des fenêtres bascule lorsque vous créez ou mettez à jour un mappage de source d'événement. Pour configurer une fenêtre variable, spécifiez la fenêtre en secondes (TumblingWindowInSeconds). L'exemple de commande suivant AWS Command Line Interface (AWS CLI) crée un mappage des sources d'événements de streaming dont la fenêtre de basculement est de 120 secondes. La fonction d'événement Lambda définie pour l'agrégation et le traitement est nommée. `tumbling-window-example-function`

```
aws lambda create-event-source-mapping \
--event-source-arn arn:aws:dynamodb:us-east-2:123456789012:table/my-table/
stream/2024-06-10T19:26:16.525 \
--function-name tumbling-window-example-function \
--starting-position TRIM_HORIZON \
```

```
--tumbling-window-in-seconds 120
```

Lambda détermine les limites des fenêtres bascule en fonction de l'heure à laquelle les enregistrements ont été insérés dans le flux. Tous les enregistrements ont un horodatage approximatif disponible que Lambda utilise pour déterminer des limites.

Les agrégations de fenêtres bascule ne prennent pas en charge le repartitionnement. Quand la partition prend fin, Lambda considère que la fenêtre de traitement est fermée, et les partitions enfants entament leur propre fenêtre de traitement dans un nouvel état.

Les fenêtres bascule prennent complètement en charge les stratégies de nouvelle tentative existantes `maxRetryAttempts` et `maxRecordAge`.

Example Handler.py — Agrégation et traitement

La fonction Python suivante montre comment regrouper et traiter votre état final :

```
def lambda_handler(event, context):
    print('Incoming event: ', event)
    print('Incoming state: ', event['state'])

#Check if this is the end of the window to either aggregate or process.
    if event['isFinalInvokeForWindow']:
        # logic to handle final state of the window
        print('Destination invoke')
    else:
        print('Aggregate invoke')

#Check for early terminations
    if event['isWindowTerminatedEarly']:
        print('Window terminated early')

    #Aggregation logic
    state = event['state']
    for record in event['Records']:
        state[record['dynamodb']['NewImage']['Id']] = state.get(record['dynamodb']
['NewImage']['Id'], 0) + 1

    print('Returning state: ', state)
    return {'state': state}
```

Paramètres Lambda pour les mappages des sources d’événement Amazon DynamoDB

Tous les types de sources d'événements Lambda partagent les mêmes opérations CreateEventSourceMappinget les mêmes opérations d'UpdateEventSourceMappingAPI. Cependant, seuls certains paramètres s’appliquent à DynamoDB Streams.

Paramètre	Obligatoire	Par défaut	Remarques
BatchSize	N	100	Maximum : 10 000.
BisectBatchOnFunctionError	N	FAUX	Aucune
DestinationConfig	N	N/A	File d’attente Amazon SQS standard ou destination de rubrique Amazon SNS standard pour les enregistrements ignorés
Activé	N	VRAI	Aucune
EventSourceArn	Y	N/A	ARN du flux de données ou d’un consommateur de flux
FilterCriteria	N	N/A	Contrôlez les événements que Lambda envoie à votre fonction d'événement
FunctionName	O	N/A	Aucune
FunctionResponseTypes	N	N/A	Pour permettre à votre fonction de signaler des échecs

Paramètre	Obligatoire	Par défaut	Remarques
			spécifiques dans un lot, incluez la valeur `ReportBatchItemFailures` dans `FunctionResponseTypes`. Pour plus d'informations, consultez Configuration d'une réponse par lots partielle avec DynamoDB et Lambda.
MaximumBatchingWindowInSeconds	N	0	Aucune
MaximumRecordAgeInSeconds	N	-1	-1 signifie infini : les enregistrements qui ont échoué sont réessayés jusqu'à ce que l'enregistrement expire. La limite de conservation des données pour les flux DynamoDB est de 24 heures. Minimum : -1 Maximum : 604 800

Paramètre	Obligatoire	Par défaut	Remarques
MaximumRetryAttempts	N	-1	-1 signifie infini : les registres qui ont échoué sont réessayés jusqu'à ce que le registre expire. Minimum : 0 Maximum : 10 000.
ParallelizationFactor	N	1	Maximum : 10
StartingPosition	O	N/A	TRIM_HORIZON ou LATEST
TumblingWindowInSeconds	N	N/A	Minimum : 0 Maximum : 900

Utilisation du filtrage des événements avec une source d'événement DynamoDB

Vous pouvez utiliser le filtrage des événements pour contrôler les enregistrements d'un flux ou d'une file d'attente que Lambda envoie à votre fonction d'événement. Pour obtenir des informations générales sur le fonctionnement du filtrage des événements, consultez the section called "Filtrage des événements".

Cette section porte sur le filtrage des événements pour les sources d'événement DynamoDB.

> **Note**
>
> Les mappages des sources d'événements DynamoDB prennent uniquement en charge le filtrage sur la clé `dynamodb`.

Rubriques

- Événement DynamoDB
- Filtrage à l'aide des attributs de table

- Filtrage à l'aide d'expressions booléennes
- Utilisation de l'opérateur Exists
- Format JSON pour le filtrage DynamoDB

Événement DynamoDB

Supposons que vous ayez une table DynamoDB avec la clé primaire `CustomerName` et les attributs `AccountManager` et `PaymentTerms`. Voici un exemple d'enregistrement issu du flux de votre table DynamoDB.

```
{
      "eventID": "1",
      "eventVersion": "1.0",
      "dynamodb": {
          "ApproximateCreationDateTime": "1678831218.0",
          "Keys": {
              "CustomerName": {
                  "S": "AnyCompany Industries"
              }
          },
          "NewImage": {
              "AccountManager": {
                  "S": "Pat Candella"
              },
              "PaymentTerms": {
                  "S": "60 days"
              },
              "CustomerName": {
                  "S": "AnyCompany Industries"
              }
          },
          "SequenceNumber": "111",
          "SizeBytes": 26,
          "StreamViewType": "NEW_IMAGE"
      }
  }
```

Pour filtrer sur la base des valeurs de clé et d'attribut de votre table DynamoDB, utilisez la clé `dynamodb` dans l'enregistrement. Les sections suivantes fournissent des exemples de différents types de filtres.

Filtrage à l'aide des clés de table

Supposons que vous souhaitiez que votre fonction événementielle traite uniquement les enregistrements dont la clé primaire `CustomerName` est « AnyCompany Industries ». L'objet `FilterCriteria` serait le suivant.

```
{
     "Filters": [
          {
              "Pattern": "{ \"dynamodb\" : { \"Keys\" : { \"CustomerName\" : { \"S\" :
 [ \"AnyCompany Industries\" ] } } } }"
          }
      ]
 }
```

Pour plus de clarté, voici la valeur du `Pattern` de filtre étendu en JSON simple :

```
{
     "dynamodb": {
          "Keys": {
              "CustomerName": {
                  "S": [ "AnyCompany Industries" ]
                  }
              }
          }
 }
```

Vous pouvez ajouter votre filtre à l'aide de la console AWS CLI ou d'un AWS SAM modèle.

Console

Pour ajouter ce filtre à l'aide de la console, suivez les instructions de Attacher des critères de filtre à un mappage de sources d'événements (console) et saisissez la chaîne suivante comme critère de filtre.

```
{ "dynamodb" : { "Keys" : { "CustomerName" : { "S" : [ "AnyCompany
 Industries" ] } } } }
```

AWS CLI

Pour créer un nouveau mappage de source d'événements avec ces critères de filtre à l'aide de AWS Command Line Interface (AWS CLI), exécutez la commande suivante.

```
aws lambda create-event-source-mapping \
    --function-name my-function \
    --event-source-arn arn:aws:dynamodb:us-east-2:123456789012:table/my-table \
    --filter-criteria '{"Filters": [{"Pattern": "{ \"dynamodb\" : { \"Keys\" :
 { \"CustomerName\" : { \"S\" : [ \"AnyCompany Industries\" ] } } } }"}]}'
```

Pour ajouter ces critères de filtre à un mappage des sources d'événements existant, exécutez la commande suivante.

```
aws lambda update-event-source-mapping \
    --uuid "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE" \
    --filter-criteria '{"Filters": [{"Pattern": "{ \"dynamodb\" : { \"Keys\" :
 { \"CustomerName\" : { \"S\" : [ \"AnyCompany Industries\" ] } } } }"}]}'
```

AWS SAM

Pour ajouter ce filtre AWS SAM, ajoutez l'extrait suivant au modèle YAML de votre source d'événement.

```
FilterCriteria:
   Filters:
     - Pattern: '{ "dynamodb" : { "Keys" : { "CustomerName" : { "S" : [ "AnyCompany
 Industries" ] } } } }'
```

Filtrage à l'aide des attributs de table

Avec DynamoDB, vous pouvez également utiliser les clés `NewImage` et `OldImage` pour filtrer les valeurs d'attributs. Supposons que vous souhaitiez filtrer les enregistrements dont l'`AccountManager`attribut dans la dernière image de table est « Pat Candella » ou « Shirley Rodriguez ». L'objet `FilterCriteria` serait le suivant.

```
{
    "Filters": [
        {
            "Pattern": "{ \"dynamodb\" : { \"NewImage\" : { \"AccountManager\" : { \"S
\" : [ \"Pat Candella\", \"Shirley Rodriguez\" ] } } } }"
        }
    ]
}
```

Pour plus de clarté, voici la valeur du `Pattern` de filtre étendu en JSON simple :

```
{
    "dynamodb": {
        "NewImage": {
            "AccountManager": {
                "S": [ "Pat Candella", "Shirley Rodriguez" ]
            }
        }
    }
}
```

Vous pouvez ajouter votre filtre à l'aide de la console AWS CLI ou d'un AWS SAM modèle.

Console

Pour ajouter ce filtre à l'aide de la console, suivez les instructions de Attacher des critères de filtre à un mappage de sources d'événements (console) et saisissez la chaîne suivante comme critère de filtre.

```
{ "dynamodb" : { "NewImage" : { "AccountManager" : { "S" : [ "Pat Candella",
 "Shirley Rodriguez" ] } } } }
```

AWS CLI

Pour créer un nouveau mappage de source d'événements avec ces critères de filtre à l'aide de AWS Command Line Interface (AWS CLI), exécutez la commande suivante.

```
aws lambda create-event-source-mapping \
    --function-name my-function \
    --event-source-arn arn:aws:dynamodb:us-east-2:123456789012:table/my-table \
    --filter-criteria '{"Filters": [{"Pattern": "{ \"dynamodb\" : { \"NewImage
\" : { \"AccountManager\" : { \"S\" : [ \"Pat Candella\", \"Shirley Rodriguez
\" ] } } } }"}]}'
```

Pour ajouter ces critères de filtre à un mappage des sources d'événements existant, exécutez la commande suivante.

```
aws lambda update-event-source-mapping \
    --uuid "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE" \
```

```
    --filter-criteria '{"Filters": [{"Pattern": "{ \"dynamodb\" : { \"NewImage
\" : { \"AccountManager\" : { \"S\" : [ \"Pat Candella\", \"Shirley Rodriguez
\" ] } } } }"}]}'
```

AWS SAM

Pour ajouter ce filtre AWS SAM, ajoutez l'extrait suivant au modèle YAML de votre source d'événement.

```
FilterCriteria:
  Filters:
    - Pattern: '{ "dynamodb" : { "NewImage" : { "AccountManager" : { "S" : [ "Pat
 Candella", "Shirley Rodriguez" ] } } } }'
```

Filtrage à l’aide d’expressions booléennes

Vous pouvez également créer des filtres à l’aide des expressions booléennes AND. Ces expressions peuvent inclure les paramètres de clé et d’attribut de votre table. Supposons que vous souhaitiez filtrer les enregistrements dont la valeur `NewImage` d’`AccountManager` est « Pat Candella » et la valeur `OldImage` est « Terry Whitlock ». L’objet `FilterCriteria` serait le suivant.

```
{
    "Filters": [
        {
            "Pattern": "{ \"dynamodb\" : { \"NewImage\" : { \"AccountManager\" : { \"S
\" : [ \"Pat Candella\" ] } } } , \"dynamodb\" : { \"OldImage\" : { \"AccountManager
\" : { \"S\" : [ \"Terry Whitlock\" ] } } } }"
        }
    ]
}
```

Pour plus de clarté, voici la valeur du `Pattern` de filtre étendu en JSON simple :

```
{
    "dynamodb" : {
        "NewImage" : {
            "AccountManager" : {
                "S" : [
                    "Pat Candella"
                ]
            }
```

```
        }
    },
    "dynamodb": {
        "OldImage": {
            "AccountManager": {
                "S": [
                    "Terry Whitlock"
                ]
            }
        }
    }
}
```

Vous pouvez ajouter votre filtre à l'aide de la console AWS CLI ou d'un AWS SAM modèle.

Console

Pour ajouter ce filtre à l'aide de la console, suivez les instructions de Attacher des critères de filtre à un mappage de sources d'événements (console) et saisissez la chaîne suivante comme critère de filtre.

```
{ "dynamodb" : { "NewImage" : { "AccountManager" : { "S" : [ "Pat
 Candella" ] } } } , "dynamodb" : { "OldImage" : { "AccountManager" : { "S" :
 [ "Terry Whitlock" ] } } } }
```

AWS CLI

Pour créer un nouveau mappage de source d'événements avec ces critères de filtre à l'aide de AWS Command Line Interface (AWS CLI), exécutez la commande suivante.

```
aws lambda create-event-source-mapping \
    --function-name my-function \
    --event-source-arn arn:aws:dynamodb:us-east-2:123456789012:table/my-table \
    --filter-criteria '{"Filters": [{"Pattern": "{ \"dynamodb\" : { \"NewImage
\" : { \"AccountManager\" : { \"S\" : [ \"Pat Candella\" ] } } } , \"dynamodb\" :
 { \"OldImage\" : { \"AccountManager\" : { \"S\" : [ \"Terry Whitlock\" ] } } } }
 "}]}'
```

Pour ajouter ces critères de filtre à un mappage des sources d'événements existant, exécutez la commande suivante.

```
aws lambda update-event-source-mapping \
```

```
    --uuid "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE" \
    --filter-criteria '{"Filters": [{"Pattern": "{ \"dynamodb\" : { \"NewImage
\" : { \"AccountManager\" : { \"S\" : [ \"Pat Candella\" ] } } } , \"dynamodb\" :
 { \"OldImage\" : { \"AccountManager\" : { \"S\" : [ \"Terry Whitlock\" ] } } } }
 "}]}'
```

AWS SAM

Pour ajouter ce filtre AWS SAM, ajoutez l'extrait suivant au modèle YAML de votre source d'événement.

```
FilterCriteria:
  Filters:
    - Pattern: '{ "dynamodb" : { "NewImage" : { "AccountManager" : { "S" : [ "Pat
 Candella" ] } } } , "dynamodb" : { "OldImage" : { "AccountManager" : { "S" :
 [ "Terry Whitlock" ] } } } }'
```

> **Note**
>
> Le filtrage des événements DynamoDB ne prend pas en charge l'utilisation d'opérateurs numériques (valeurs numériques égales et plage numérique). Même si les éléments de votre table sont stockés sous forme de nombres, ces paramètres sont convertis en chaînes dans l'objet d'enregistrement JSON.

Utilisation de l'opérateur Exists

En raison de la structure des objets d'événements JSON de DynamoDB, l'utilisation de l'opérateur Exists nécessite une attention particulière. L'opérateur Exists ne fonctionne que sur les nœuds terminaux dans l'événement JSON. Par conséquent, si votre modèle de filtre utilise Exists pour tester un nœud intermédiaire, il ne fonctionnera pas. Observez l'élément de table DynamoDB suivant :

```
{
  "UserID": {"S": "12345"},
  "Name": {"S": "John Doe"},
  "Organizations": {"L": [
      {"S":"Sales"},
      {"S":"Marketing"},
      {"S":"Support"}
    ]
```

```
  }
}
```

Vous pourriez avoir besoin de créer un modèle de filtre comme le suivant pour tester les événements contenant `"Organizations"` :

```
{ "dynamodb" : { "NewImage" : { "Organizations" : [ { "exists": true } ] } } }
```

Cependant, ce modèle de filtre ne renverra jamais de correspondance, car `"Organizations"` n'est pas un nœud terminal. L'exemple suivant montre comment utiliser correctement l'opérateur Exists pour construire le modèle de filtre souhaité :

```
{ "dynamodb" : { "NewImage" : {"Organizations": {"L": {"S": [ {"exists":
 true } ] } } } } }
```

Format JSON pour le filtrage DynamoDB

Pour filtrer correctement les événements provenant de sources DynamoDB, le champ de données et vos critères de filtre pour le champ de données (`dynamodb`) doivent être au format JSON valide. Si l'un ou l'autre des champs n'est pas dans un format JSON valide, Lambda rejette le message ou lance une exception. Le tableau suivant résume le comportement spécifique :

Format des données entrantes	Pas de modèle de filtre pour les propriétés des données	Action obtenue.
JSON valide	JSON valide	Lambda filtre en fonction de vos critères de filtre.
JSON valide	Pas de modèle de filtre pour les propriétés des données	Lambda filtre (uniquement selon les autres propriétés de métadonnées) en fonction de vos critères de filtre.
JSON valide	Non-JSON	Lambda lance une exception au moment de la création ou de la mise à jour du mappage de sources d'événements. Le modèle de filtre des propriétés

Format des données entrantes	Pas de modèle de filtre pour les propriétés des données	Action obtenue.
		de données doit être au format JSON valide.
Non-JSON	JSON valide	Lambda rejette l'enregis trement.
Non-JSON	Pas de modèle de filtre pour les propriétés des données	Lambda filtre (uniquement selon les autres propriétés de métadonnées) en fonction de vos critères de filtre.
Non-JSON	Non-JSON	Lambda lance une exception au moment de la création ou de la mise à jour du mappage de sources d'événements. Le modèle de filtre des propriétés de données doit être au format JSON valide.

Tutoriel : Utilisation AWS Lambda avec les flux Amazon DynamoDB

Dans ce didacticiel, vous allez créer une fonction d'événement Lambda pour utiliser les événements d'un flux Amazon DynamoDB.

Conditions préalables

Installer la AWS Command Line Interface

Si vous ne l'avez pas encore installé AWS Command Line Interface, suivez les étapes décrites dans la section Installation ou mise à jour de la dernière version du AWS CLI pour l'installer.

Ce tutoriel nécessite un terminal de ligne de commande ou un shell pour exécuter les commandes. Sous Linux et macOS, utilisez votre gestionnaire de shell et de package préféré.

> **Note**
>
> Sous Windows, certaines commandes CLI Bash que vous utilisez couramment avec Lambda (par exemple `zip`) ne sont pas prises en charge par les terminaux intégrés du système d'exploitation. Pour obtenir une Windows-integrated version d'Ubuntu et de Bash, installez le sous-système Windows pour Linux.

Créer le rôle d'exécution

Créez le rôle d'exécution qui autorise votre fonction à accéder aux AWS ressources.

Pour créer un rôle d'exécution

1. Ouvrez la page Roles (Rôles) dans la console IAM.
2. Sélectionnez Créer un rôle.
3. Créez un rôle avec les propriétés suivantes :
   - Entité de confiance – Lambda.
   - Autorisations — AWSLambdaDynamoDBExecutionRole.
   - Nom de rôle – **`lambda-dynamodb-role`**.

AWSLambdaDynamoDBExecutionRoleDispose des autorisations nécessaires à la fonction pour lire des éléments depuis DynamoDB et écrire des journaux dans Logs. CloudWatch

Création de la fonction d'événement

Créez une fonction d'événement Lambda qui traite vos événements DynamoDB. Le code de fonction écrit certaines des données d'événements entrants dans CloudWatch Logs.

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement DynamoDB avec Lambda en utilisant .NET.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
using System.Text.Json;
using System.Text;
using Amazon.Lambda.Core;
using Amazon.Lambda.DynamoDBEvents;

// Assembly attribute to enable the Lambda function's JSON input to be converted
 into a .NET class.
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSeri

namespace AWSLambda_DDB;

public class Function
{
    public void FunctionHandler(DynamoDBEvent dynamoEvent, ILambdaContext
 context)
    {
        context.Logger.LogInformation($"Beginning to process
 {dynamoEvent.Records.Count} records...");

        foreach (var record in dynamoEvent.Records)
        {
            context.Logger.LogInformation($"Event ID: {record.EventID}");
            context.Logger.LogInformation($"Event Name: {record.EventName}");

            context.Logger.LogInformation(JsonSerializer.Serialize(record));
        }

        context.Logger.LogInformation("Stream processing complete.");
    }
}
```

Go

Kit SDK pour Go V2

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement DynamoDB avec Lambda en utilisant Go.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package main

import (
 "context"
 "github.com/aws/aws-lambda-go/lambda"
 "github.com/aws/aws-lambda-go/events"
 "fmt"
)

func HandleRequest(ctx context.Context, event events.DynamoDBEvent) (*string,
 error) {
 if len(event.Records) == 0 {
  return nil, fmt.Errorf("received empty event")
 }

 for _, record := range event.Records {
   LogDynamoDBRecord(record)
 }

 message := fmt.Sprintf("Records processed: %d", len(event.Records))
 return &message, nil
}

func main() {
 lambda.Start(HandleRequest)
}

func LogDynamoDBRecord(record events.DynamoDBEventRecord){
 fmt.Println(record.EventID)
```

```
 fmt.Println(record.EventName)
 fmt.Printf("%+v\n", record.Change)
}
```

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement DynamoDB avec Lambda en utilisant Java.

```
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.DynamodbEvent;
import
 com.amazonaws.services.lambda.runtime.events.DynamodbEvent.DynamodbStreamRecord;
import com.google.gson.Gson;
import com.google.gson.GsonBuilder;

public class example implements RequestHandler<DynamodbEvent, Void> {

    private static final Gson GSON = new
 GsonBuilder().setPrettyPrinting().create();

    @Override
    public Void handleRequest(DynamodbEvent event, Context context) {
        System.out.println(GSON.toJson(event));
        event.getRecords().forEach(this::logDynamoDBRecord);
        return null;
    }

    private void logDynamoDBRecord(DynamodbStreamRecord record) {
        System.out.println(record.getEventID());
        System.out.println(record.getEventName());
        System.out.println("DynamoDB Record: " +
 GSON.toJson(record.getDynamodb()));
    }
```

```
}
```

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement DynamoDB avec Lambda en utilisant. JavaScript

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
exports.handler = async (event, context) => {
    console.log(JSON.stringify(event, null, 2));
    event.Records.forEach(record => {
        logDynamoDBRecord(record);
    });
};

const logDynamoDBRecord = (record) => {
    console.log(record.eventID);
    console.log(record.eventName);
    console.log(`DynamoDB Record: ${JSON.stringify(record.dynamodb)}`);
};
```

Consommation d'un événement DynamoDB avec Lambda en utilisant. TypeScript

```
export const handler = async (event, context) => {
    console.log(JSON.stringify(event, null, 2));
    event.Records.forEach(record => {
        logDynamoDBRecord(record);
    });
}
const logDynamoDBRecord = (record) => {
    console.log(record.eventID);
    console.log(record.eventName);
```

```
    console.log(`DynamoDB Record: ${JSON.stringify(record.dynamodb)}`);
};
```

PHP

Kit SDK pour PHP

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement DynamoDB avec Lambda en utilisant PHP.

```
<?php

# using bref/bref and bref/logger for simplicity

use Bref\Context\Context;
use Bref\Event\DynamoDb\DynamoDbEvent;
use Bref\Event\DynamoDb\DynamoDbHandler;
use Bref\Logger\StderrLogger;

require __DIR__ . '/vendor/autoload.php';

class Handler extends DynamoDbHandler
{
    private StderrLogger $logger;

    public function __construct(StderrLogger $logger)
    {
        $this->logger = $logger;
    }

    /**
     * @throws JsonException
     * @throws \Bref\Event\InvalidLambdaEvent
     */
    public function handleDynamoDb(DynamoDbEvent $event, Context $context): void
    {
        $this->logger->info("Processing DynamoDb table items");
```

```
        $records = $event->getRecords();

        foreach ($records as $record) {
            $eventName = $record->getEventName();
            $keys = $record->getKeys();
            $old = $record->getOldImage();
            $new = $record->getNewImage();

            $this->logger->info("Event Name:".$eventName."\n");
            $this->logger->info("Keys:". json_encode($keys)."\n");
            $this->logger->info("Old Image:". json_encode($old)."\n");
            $this->logger->info("New Image:". json_encode($new));

            // TODO: Do interesting work based on the new data

            // Any exception thrown will be logged and the invocation will be
 marked as failed
        }

        $totalRecords = count($records);
        $this->logger->info("Successfully processed $totalRecords items");
    }
}

$logger = new StderrLogger();
return new Handler($logger);
```

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement DynamoDB avec Lambda en utilisant Python.

```
import json
```

```
def lambda_handler(event, context):
    print(json.dumps(event, indent=2))

    for record in event['Records']:
        log_dynamodb_record(record)

def log_dynamodb_record(record):
    print(record['eventID'])
    print(record['eventName'])
    print(f"DynamoDB Record: {json.dumps(record['dynamodb'])}")
```

Ruby

Kit SDK pour Ruby

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement DynamoDB avec Lambda en utilisant Ruby.

```
def lambda_handler(event:, context:)
    return 'received empty event' if event['Records'].empty?

    event['Records'].each do |record|
      log_dynamodb_record(record)
    end

    "Records processed: #{event['Records'].length}"
  end

  def log_dynamodb_record(record)
    puts record['eventID']
    puts record['eventName']
    puts "DynamoDB Record: #{JSON.generate(record['dynamodb'])}"
  end
```

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement DynamoDB avec Lambda en utilisant Rust.

```
use lambda_runtime::{service_fn, tracing, Error, LambdaEvent};
use aws_lambda_events::{
    event::dynamodb::{Event, EventRecord},
   };


// Built with the following dependencies:
//lambda_runtime = "0.11.1"
//serde_json = "1.0"
//tokio = { version = "1", features = ["macros"] }
//tracing = { version = "0.1", features = ["log"] }
//tracing-subscriber = { version = "0.3", default-features = false, features =
 ["fmt"] }
//aws_lambda_events = "0.15.0"

async fn function_handler(event: LambdaEvent<Event>) ->Result<(), Error> {

    let records = &event.payload.records;
    tracing::info!("event payload: {:?}",records);
    if records.is_empty() {
        tracing::info!("No records found. Exiting.");
        return Ok(());
    }

    for record in records{
        log_dynamo_dbrecord(record);
    }

    tracing::info!("Dynamo db records processed");
```

```
    // Prepare the response
    Ok(())

}

fn log_dynamo_dbrecord(record: &EventRecord)-> Result<(), Error>{
    tracing::info!("EventId: {}", record.event_id);
    tracing::info!("EventName: {}", record.event_name);
    tracing::info!("DynamoDB Record: {:?}", record.change );
    Ok(())

}

#[tokio::main]
async fn main() -> Result<(), Error> {
    tracing_subscriber::fmt()
    .with_max_level(tracing::Level::INFO)
    .with_target(false)
    .without_time()
    .init();

    let func = service_fn(function_handler);
    lambda_runtime::run(func).await?;
    Ok(())

}
```

Pour créer la fonction d'événement

1. Copiez l'exemple de code dans un fichier nommé `example.js`.
2. Créez un package de déploiement.

```
zip function.zip example.js
```

3. Créez une fonction d'événement Lambda à l'aide de la `create-function` commande.

```
aws lambda create-function --function-name ProcessDynamoDBRecords \
    --zip-file fileb://function.zip --handler example.handler --runtime nodejs24.x
 \
    --role arn:aws:iam::111122223333:role/lambda-dynamodb-role
```

Tester la fonction d'événement Lambda

Au cours de cette étape, vous appelez manuellement votre fonction d'événement Lambda à l'aide de la commande `invoke` AWS Lambda CLI et de l'exemple d'événement DynamoDB suivant. Copiez le code suivant dans un fichier nommé `input.txt`.

Example input.txt

```
{
   "Records":[
      {
         "eventID":"1",
         "eventName":"INSERT",
         "eventVersion":"1.0",
         "eventSource":"aws:dynamodb",
         "awsRegion":"us-east-1",
         "dynamodb":{
            "Keys":{
               "Id":{
                  "N":"101"
               }
            },
            "NewImage":{
               "Message":{
                  "S":"New item!"
               },
               "Id":{
                  "N":"101"
               }
            },
            "SequenceNumber":"111",
            "SizeBytes":26,
            "StreamViewType":"NEW_AND_OLD_IMAGES"
         },
         "eventSourceARN":"stream-ARN"
      },
      {
         "eventID":"2",
         "eventName":"MODIFY",
         "eventVersion":"1.0",
         "eventSource":"aws:dynamodb",
         "awsRegion":"us-east-1",
         "dynamodb":{
```

```
            "Keys":{
               "Id":{
                  "N":"101"
               }
            },
            "NewImage":{
               "Message":{
                  "S":"This item has changed"
               },
               "Id":{
                  "N":"101"
               }
            },
            "OldImage":{
               "Message":{
                  "S":"New item!"
               },
               "Id":{
                  "N":"101"
               }
            },
            "SequenceNumber":"222",
            "SizeBytes":59,
            "StreamViewType":"NEW_AND_OLD_IMAGES"
         },
         "eventSourceARN":"stream-ARN"
      },
      {
         "eventID":"3",
         "eventName":"REMOVE",
         "eventVersion":"1.0",
         "eventSource":"aws:dynamodb",
         "awsRegion":"us-east-1",
         "dynamodb":{
            "Keys":{
               "Id":{
                  "N":"101"
               }
            },
            "OldImage":{
               "Message":{
                  "S":"This item has changed"
               },
               "Id":{
```

```
                    "N":"101"
                 }
              },
              "SequenceNumber":"333",
              "SizeBytes":38,
              "StreamViewType":"NEW_AND_OLD_IMAGES"
           },
           "eventSourceARN":"stream-ARN"
        }
    ]
}
```

Exécutez la commande suivante `invoke`.

```
aws lambda invoke --function-name ProcessDynamoDBRecords \
    --cli-binary-format raw-in-base64-out \
    --payload file://input.txt outputfile.txt
```

L'cli-binary-formatoption est obligatoire si vous utilisez AWS CLI la version 2. Pour faire de ce paramètre le paramètre par défaut, exécutez `aws configure set cli-binary-format raw-in-base64-out`. Pour plus d'informations, consultez les options de ligne de commande globales prises en charge par l'AWS CLI dans le Guide de l'utilisateur AWS Command Line Interface version 2.

La fonction renvoie la chaîne `message` dans le corps de la réponse.

Vérifiez la sortie dans le fichier `outputfile.txt`.

Créer une table DynamoDB avec un flux activé

Créez une table Amazon DynamoDB avec un flux activé.

Pour créer une table DynamoDB

1. Ouvrez la console DynamoDB.
2. Choisissez Créer un tableau.
3. Créez une table avec les paramètres suivants.
   - Nom de la table – **`lambda-dynamodb-stream`**
   - Clé primaire – **`id`** (chaîne)
4. Choisissez Create (Créer).

Pour activer les flux

1. Ouvrez la console DynamoDB.
2. Choisissez Tables.
3. Choisissez la table lambda-dynamodb-stream.
4. Sous la section Exports and streams (Exportations et flux), choisissez DynamoDB stream details (Détails du flux DynamoDB).
5. Choisissez Activer.
6. Pour Type de vue, sélectionnez Attributs de clé uniquement.
7. Choisissez Activer le streaming.

Écrivez l'ARN du flux. Vous en aurez besoin à l'étape suivante lorsque vous associerez le flux à votre fonction d'événement Lambda. Pour plus d'informations sur l'activation des flux, consultez Capture d'activité Table avec DynamoDB Streams.

Ajouter une source d'événement dans AWS Lambda

Créez un mappage de source d'événement dans AWS Lambda. Ce mappage des sources d'événements associe le flux DynamoDB à votre fonction d'événement Lambda. Après avoir créé ce mappage des sources d'événements, AWS Lambda commence à interroger le flux.

Exécutez la commande suivante AWS CLI `create-event-source-mapping`. Une fois la commande exécutée, notez l'UUID. Vous aurez besoin de l'UUID pour faire référence au mappage de source d'événement dans les commandes (par exemple, lors de la suppression du mappage).

```
aws lambda create-event-source-mapping --function-name ProcessDynamoDBRecords \
    --batch-size 100 --starting-position LATEST --event-source DynamoDB-stream-arn
```

Cela crée un mappage entre le flux DynamoDB spécifié et la fonction d'événement Lambda. Vous pouvez associer un flux DynamoDB à plusieurs fonctions d'événement Lambda et associer la même fonction d'événement Lambda à plusieurs flux. Cependant, les fonctions d'événement Lambda partagent le débit de lecture du flux qu'elles partagent.

Pour obtenir la liste des mappages de source d'événement, exécutez la commande suivante.

```
aws lambda list-event-source-mappings
```

Cette liste renvoie tous les mappages de source d'événement que vous avez créés et indique la valeur `LastProcessingResult` pour chacun d'eux, entre autres. Ce champ est utilisé pour fournir un message d'information en cas de problème. Des valeurs telles que `No records processed` (indique que le sondage n' AWS Lambda a pas commencé ou qu'il n'y a aucun enregistrement dans le flux) et `OK` (indique que les enregistrements du flux AWS Lambda ont été lus avec succès et que votre fonction d'événement Lambda a invoqué votre fonction d'événement Lambda) indiquent qu'il n'y a aucun problème. Dans le cas contraire, vous recevez un message d'erreur.

Si vous avez un grand nombre de mappages de source d'événement, utilisez le paramètre du nom de la fonction pour affiner les résultats.

```
aws lambda list-event-source-mappings --function-name ProcessDynamoDBRecords
```

Tester la configuration

Testez l'environnement complet. A mesure que vous mettez la table à jour, DynamoDB écrit les enregistrements d'événement dans le flux. Lorsqu'il AWS Lambda interroge le flux, il détecte les nouveaux enregistrements dans le flux et invoque votre fonction d'événement Lambda en votre nom en transmettant des événements à la fonction.

1. Dans la console DynamoDB, vous pouvez ajouter, mettre à jour et supprimer des éléments dans la table. DynamoDB écrit des enregistrements de ces actions dans le flux.
2. AWS Lambda interroge le flux et lorsqu'il détecte des mises à jour du flux, il invoque votre fonction d'événement Lambda en transmettant les données d'événement qu'il trouve dans le flux.
3. Votre fonction s'exécute et crée des journaux sur Amazon CloudWatch. Vous pouvez vérifier les journaux signalés dans la CloudWatch console Amazon.

Étapes suivantes

Ce didacticiel vous a montré les principes de base du traitement des événements de flux DynamoDB avec Lambda. Pour les charges de travail de production, envisagez de mettre en œuvre une logique de réponse partielle de lot afin de gérer plus efficacement les échecs d'enregistrement individuels. L'utilitaire de traitement par lots de Powertools for AWS Lambda est disponible en Python TypeScript, .NET et Java et fournit une solution robuste pour cela, en gérant automatiquement la complexité des réponses partielles par lots et en réduisant le nombre de tentatives pour les enregistrements traités avec succès.

Nettoyage de vos ressources

Vous pouvez maintenant supprimer les ressources que vous avez créées pour ce didacticiel, sauf si vous souhaitez les conserver. En supprimant AWS les ressources que vous n'utilisez plus, vous évitez des frais inutiles pour votre Compte AWS.

Pour supprimer la fonction d'événement Lambda

1. Ouvrez la page Event Functions de la console Lambda.
2. Sélectionnez la fonction d'événement que vous avez créée.
3. Sélectionnez Actions, Supprimer.
4. Saisissez **`confirm`** dans la zone de saisie de texte et choisissez Delete (Supprimer).

Pour supprimer le rôle d’exécution

1. Ouvrez la page Roles (Rôles) de la console IAM.
2. Sélectionnez le rôle d’exécution que vous avez créé.
3. Sélectionnez Supprimer.
4. Saisissez le nom du rôle dans le champ de saisie de texte et choisissez Delete (Supprimer).

Pour supprimer la table DynamoDB

1. Ouvrez la page Tables (Tables) de la console DynamoDB.
2. Sélectionnez la table que vous avez créée.
3. Choisissez Supprimer.
4. Saisissez **`delete`** dans la zone de texte.
5. Choisissez Supprimer la table.

Traitez les événements du cycle de vie d'Amazon EC2 avec une fonction d'événement Lambda

Vous pouvez l'utiliser AWS Lambda pour traiter les événements du cycle de vie depuis Amazon Elastic Compute Cloud et gérer les ressources Amazon EC2. Amazon EC2 envoie des événements à Amazon EventBridge (CloudWatch Events) pour des événements du cycle de vie, tels que lorsqu'une instance change d'état, lorsqu'un instantané du volume Amazon Elastic Block Store est terminé ou lorsqu'il est prévu de mettre fin à une instance Spot. Vous configurez EventBridge (CloudWatch Events) pour transmettre ces événements à une fonction d'événement Lambda pour traitement.

EventBridge (CloudWatch Events) invoque votre fonction d'événement Lambda de manière asynchrone avec le document d'événement d'Amazon EC2.

Exampleévénement du cycle de vie d’une instance

```
{
    "version": "0",
    "id": "b6ba298a-7732-2226-xmpl-976312c1a050",
    "detail-type": "EC2 Instance State-change Notification",
    "source": "aws.ec2",
    "account": "111122223333",
    "time": "2019-10-02T17:59:30Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:111122223333:instance/i-0c314xmplcd5b8173"
    ],
    "detail": {
        "instance-id": "i-0c314xmplcd5b8173",
        "state": "running"
    }
}
```

Pour plus d’informations sur la configuration des événements, consultez Invoquer une fonction d'événement Lambda selon un calendrier. Pour un exemple de fonction qui traite les notifications instantanées Amazon EBS, consultez EventBridge Scheduler for Amazon EBS.

Vous pouvez également utiliser le AWS SDK pour gérer des instances et d'autres ressources avec l'API Amazon EC2.

Octroi d'autorisations à EventBridge (CloudWatch événements)

Pour traiter les événements du cycle de vie depuis Amazon EC2, EventBridge (CloudWatch Events) a besoin d'une autorisation pour appeler votre fonction. Cette autorisation provient de la stratégie basée sur les ressourcesde la fonction. Si vous utilisez la console EventBridge (CloudWatch Events) pour configurer un déclencheur d'événement, la console met à jour la politique basée sur les ressources en votre nom. Sinon, ajoutez une instruction comme suit :

Example Déclaration de stratégie basée sur une ressource pour les notifications de cycle de vie Amazon EC2

```
{
  "Sid": "ec2-events",
  "Effect": "Allow",
  "Principal": {
    "Service": "events.amazonaws.com"
  },
  "Action": "lambda:InvokeFunction",
  "Resource": "arn:aws:lambda:us-east-1:12456789012:function:my-function",
  "Condition": {
    "ArnLike": {
      "AWS:SourceArn": "arn:aws:events:us-east-1:12456789012:rule/*"
    }
  }
}
```

Pour ajouter une instruction, utilisez la `add-permission` AWS CLI commande.

```
aws lambda add-permission --action lambda:InvokeFunction --statement-id ec2-events \
--principal events.amazonaws.com --function-name my-function --source-arn
 'arn:aws:events:us-east-1:12456789012:rule/*'
```

Si votre fonction utilise le AWS SDK pour gérer les ressources Amazon EC2, ajoutez des autorisations Amazon EC2 au rôle d'exécution de la fonction.

Traitet les demandes d’Application Load Balancer avec Lambda

Vous pouvez utiliser une fonction d'événement Lambda pour traiter les demandes provenant d'un Application Load Balancer. Elastic Load Balancing prend en charge les fonctions d'événement Lambda en tant que cible pour un Application Load Balancer. Utilisez les règles de l’équilibreur de charge pour acheminer les demandes HTTP vers une fonction, selon le chemin d’accès ou les valeurs des en-têtes. Traitez la demande et renvoyez une réponse HTTP à partir de votre fonction d'événement Lambda.

Elastic Load Balancing invoque votre fonction d'événement Lambda de manière synchrone avec un événement contenant le corps de la requête et les métadonnées.

Example Evénement de demande d’Application Load Balancer

```
{
    "requestContext": {
        "elb": {
            "targetGroupArn": "arn:aws:elasticloadbalancing:us-
east-1:123456789012:targetgroup/lambda-279XGJDqGZ5rsrHC2Fjr/49e9d65c45c6791a"
        }
    },
    "httpMethod": "GET",
    "path": "/lambda",
    "queryStringParameters": {
        "query": "1234ABCD"
    },
    "headers": {
        "accept": "text/html,application/xhtml+xml,application/xml;q=0.9,image/
webp,image/apng,*/*;q=0.8",
        "accept-encoding": "gzip",
        "accept-language": "en-US,en;q=0.9",
        "connection": "keep-alive",
        "host": "lambda-alb-123578498.us-east-1.elb.amazonaws.com",
        "upgrade-insecure-requests": "1",
        "user-agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36",
        "x-amzn-trace-id": "Root=1-5c536348-3d683b8b04734faae651f476",
        "x-forwarded-for": "72.12.164.125",
        "x-forwarded-port": "80",
        "x-forwarded-proto": "http",
        "x-imforwards": "20"
    },
```

```
    "body": "",
    "isBase64Encoded": False
}
```

Votre fonction traite l'événement et renvoie un document de réponse à l'équilibreur de charge en JSON. Elastic Load Balancing convertit le document en réponse de succès ou d'erreur HTTP, et la renvoie à l'utilisateur.

Example format du document de réponse

```
{
    "statusCode": 200,
    "statusDescription": "200 OK",
    "isBase64Encoded": False,
    "headers": {
        "Content-Type": "text/html"
    },
    "body": "<h1>Hello from Lambda!</h1>"
}
```

Pour configurer un Application Load Balancer comme déclencheur de fonction, accordez à Elastic Load Balancing l'autorisation d'exécuter la fonction, créez un groupe cible qui achemine les demandes vers la fonction, et ajoutez à l'équilibreur de charge une règle qui envoie les demandes au groupe cible.

Utilisez la commande `add-permission` pour ajouter une instruction d'autorisation à la stratégie basée sur les ressources de votre fonction.

```
aws lambda add-permission --function-name alb-function \
--statement-id load-balancer --action "lambda:InvokeFunction" \
--principal elasticloadbalancing.amazonaws.com
```

Vous devriez voir la sortie suivante:

```
{
    "Statement": "{\"Sid\":\"load-balancer\",\"Effect\":\"Allow\",\"Principal\":
{\"Service\":\"elasticloadbalancing.amazonaws.com\"},\"Action\":\"lambda:InvokeFunction
\",\"Resource\":\"arn:aws:lambda:us-west-2:123456789012:function:alb-function\"}"
}
```

Pour obtenir des instructions sur la configuration de l'écouteur de l'équilibreur de charge d'application et du groupe cible, consultez Fonctions Lambda en tant que cibles dans le Guide de l'utilisateur des Application Load Balancers.

Gestionnaire d'événements de Powertools pour AWS Lambda

Le gestionnaire d'événements du kit d'outils Powertools for AWS Lambda fournit le routage, le middleware, la configuration CORS, la génération de spécifications OpenAPI, la validation des demandes, la gestion des erreurs et d'autres fonctionnalités utiles lors de l'écriture de fonctions d'événements Lambda invoquées par un Application Load Balancer. L'utilitaire de gestionnaire d'événements est disponible pour Python. Pour plus d'informations, consultez l'API REST du gestionnaire d'événements dans la documentation de Powertools for AWS Lambda (Python).

Python

```
import requests
from requests import Response

from aws_lambda_powertools import Logger, Tracer
from aws_lambda_powertools.event_handler import ALBResolver
from aws_lambda_powertools.logging import correlation_paths
from aws_lambda_powertools.utilities.typing import LambdaContext

tracer = Tracer()
logger = Logger()
app = ALBResolver()


@app.get("/todos")
@tracer.capture_method
def get_todos():
    todos: Response = requests.get("https://jsonplaceholder.typicode.com/todos")
    todos.raise_for_status()

    # for brevity, we'll limit to the first 10 only
    return {"todos": todos.json()[:10]}


# You can continue to use other utilities just as before
@logger.inject_lambda_context(correlation_id_path=correlation_paths.APPLICATION_LOAD_BALANCER)
@tracer.capture_lambda_handler
def lambda_handler(event: dict, context: LambdaContext) -> dict:
```

```
    return app.resolve(event, context)
```

Invoquer une fonction d'événement Lambda selon un calendrier

Amazon EventBridge Scheduler est un planificateur sans serveur que vous pouvez utiliser pour créer, exécuter et gérer des tâches à partir d'un service géré centralisé. Avec EventBridge Scheduler, vous pouvez créer des plannings à l'aide d'expressions cron et rate pour les modèles récurrents, ou configurer des appels ponctuels. Vous pouvez configurer des fenêtres temporelles flexibles pour la livraison, définir des limites de nouvelles tentatives, ainsi que la durée de rétention maximale pour les événements non traités.

Lorsque vous configurez le EventBridge planificateur avec Lambda, le planificateur appelle votre fonction d'événement Lambda de EventBridge manière asynchrone. Vous pouvez créer un calendrier à partir de la console Lambda (à l'aide du flux Add trigger), de la console EventBridge Scheduler, du ou. AWS CLI CloudFormation Cette page explique comment utiliser le EventBridge planificateur pour appeler une fonction d'événement Lambda selon un calendrier.

Configurer le rôle d’exécution

Lorsque vous créez un nouveau calendrier, le EventBridge planificateur doit être autorisé à appeler son opération d'API cible en votre nom. Vous accordez ces autorisations au EventBridge Scheduler à l'aide d'un rôle d'exécution. La politique d’autorisation que vous associez au rôle d’exécution de votre planification définit les autorisations requises. Ces autorisations dépendent de l'API cible que le EventBridge Scheduler doit appeler.

Lorsque vous créez un planning à l'aide de la console Lambda ou de la console Scheduler, EventBridge EventBridge Scheduler définit automatiquement un rôle d'exécution en fonction de la cible que vous avez sélectionnée. Si vous souhaitez créer un calendrier à l'aide de l'un des SDK du EventBridge planificateur CloudFormation, vous devez disposer d'un rôle d'exécution existant qui accorde les autorisations dont le EventBridge planificateur a besoin pour appeler une cible. AWS CLI Pour plus d'informations sur la configuration manuelle d'un rôle d'exécution pour votre calendrier, consultez la section Configuration d'un rôle d'exécution dans le guide de l'utilisateur du EventBridge planificateur.

Création d'un calendrier à partir de la console Lambda

Utilisez le flux Ajouter un déclencheur dans la console Lambda pour créer un calendrier du EventBridge planificateur sans quitter la console.

Pour créer un déclencheur Scheduler à l'aide de la console Lambda

1. Ouvrez la page Event Functions de la console Lambda.

2. Choisissez la fonction que vous souhaitez programmer.
3. Dans le volet de Présentation de la fonction, choisissez Ajouter un déclencheur.
4. Dans le menu déroulant de la source du déclencheur, choisissez Scheduler.
5. Configurez les paramètres de planification :
   a. Nom du programme — Entrez le nom de votre programme.
   b. Groupe de planification : choisissez un groupe de planification ou utilisez-le`default`.
   c. Type de programme — Choisissez l'une des options suivantes :
      - One-time schedule — Invoque la fonction une fois à la date et à l'heure spécifiées.
      - Planification récurrente — Invoque la fonction à plusieurs reprises à l'aide d'une expression cron ou rate.
   d. (Facultatif) Entrez une charge utile JSON. Si vous n'entrez aucune charge utile, le EventBridge planificateur utilise un événement vide pour appeler la fonction.
   e. Configurez le rôle d'exécution. Pour que le EventBridge planificateur crée un nouveau rôle d'exécution pour vous, choisissez Créer un nouveau rôle pour ce calendrier. Ensuite, saisissez un nom pour Nom du rôle. Si vous choisissez cette option, le EventBridge planificateur crée une politique avec les autorisations requises et l'attache au rôle.
6. Choisissez Ajouter.

> **Tip**
>
> Vous pouvez également rechercher**`schedule`**, **`crontime`**, ou **`recurring`** trouver ce déclencheur dans le flux Ajouter un déclencheur.

Vous pouvez également utiliser la console du EventBridge planificateur pour créer un calendrier. Avec la console EventBridge Scheduler, vous pouvez configurer des options supplémentaires telles que des fenêtres horaires flexibles et des files d'attente de lettres mortes.

Affichage des EventBridge déclencheurs du planificateur

Tous les plannings du EventBridge planificateur ciblant votre fonction apparaissent dans la section Déclencheurs de la page de configuration des fonctions, sous l'étiquette Scheduler. Cela inclut les plannings créés à partir de l'une des sources suivantes :

- La console Lambda (Ajouter un flux de déclencheurs)
- La console du EventBridge planificateur
- Le SDK AWS CLI, CloudFormation, AWS SAM (en utilisant le type d'`ScheduleV2`événement) ou AWS CDK (en utilisant le `aws-scheduler` module)

> **Note**
>
> Si un planning utilise une clé gérée par le client pour le chiffrement avec une cible Universal Target Invocation (UTI), il se peut qu'elle n'apparaisse pas dans la liste des déclencheurs. Pour consulter ces plannings, utilisez la console du EventBridge planificateur.

Pour confirmer que EventBridge Scheduler a invoqué la fonction, consultez les journaux Amazon CloudWatch de la fonction.

Ressources connexes

Pour plus d'informations sur le EventBridge planificateur, consultez les rubriques suivantes :

- EventBridge Guide de l'utilisateur du planificateur
- EventBridge Référence de l'API Scheduler
- EventBridge Tarification du planificateur

Utilisation AWS Lambda avec AWS IoT

AWS IoT fournit une communication sécurisée entre les appareils connectés à Internet (tels que les capteurs) et le AWS cloud. Vous pouvez ainsi collecter les données de télémétrie de plusieurs périphériques, les stocker et les analyser.

Vous pouvez créer des AWS IoT règles avec lesquelles vos appareils pourront interagir Services AWS. Le moteur de AWS IoT règles fournit un SQL-based langage permettant de sélectionner les données à partir des charges utiles des messages et de les envoyer à d'autres services, tels qu'Amazon S3, Amazon DynamoDB AWS Lambda et. Vous définissez une règle pour invoquer une fonction d'événement Lambda lorsque vous souhaitez appeler un autre AWS service ou un service tiers.

Lorsqu'un message IoT entrant déclenche la règle, AWS IoT invoque votre fonction d'événement Lambda de manière asynchrone et transmet les données du message IoT à la fonction.

L'exemple suivant montre une mesure de l'humidité à partir d'un capteur de serre. Les valeurs row et pos identifient l'emplacement du capteur. Cet exemple d'événement est basé sur le type de serre indiqué dans les didacticiels sur les règles AWS IoT.

Example AWS IoT événement de message

```
{
    "row" : "10",
    "pos" : "23",
    "moisture" : "75"
}
```

Pour l'appel asynchrone, Lambda met le message en file d'attente et fait une nouvelle tentative si votre fonction renvoie une erreur. Configurez votre fonction avec une destination pour conserver les événements que votre fonction n'a pas pu traiter.

Vous devez autoriser le AWS IoT service à appeler votre fonction d'événement Lambda. Utilisez la commande `add-permission` pour ajouter une instruction d'autorisation à la stratégie basée sur les ressources de votre fonction.

> **Important**
>
> Si vous ajoutez une autorisation à un AWS IoT principal sans fournir le `source-arn` ou`source-account`, toute personne Compte AWS qui crée une règle avec votre AWS

Lambda action peut activer des règles à partir desquelles invoquer votre fonction d' AWS Lambda événement AWS IoT. Pour plus d'informations, consultez Autorisations AWS Lambda.

```
aws lambda add-permission --function-name my-function \
--statement-id iot-events --action "lambda:InvokeFunction" --principal
 iot.amazonaws.com \
--source-arn arn:aws:iot:us-east-1:123456789012:rule/my-rule \
--source-account 123456789012
```

Vous devriez voir la sortie suivante :

```
{
    "Statement": "{\"Sid\":\"iot-events\",\"Effect\":\"Allow\",\"Principal\":
{\"Service\":\"iot.amazonaws.com\"},\"Action\":\"lambda:InvokeFunction\",\"Resource
\":\"arn:aws:lambda:us-east-1:123456789012:function:my-function\",\"Condition\":
{\"ArnLike\":{\"AWS:SourceArn\":\"arn:aws:iot:us-east-1:123456789012:rule/my-rule\"},
\"StringEquals\":{\"AWS:SourceAccount\":\"123456789012\"}}}"
}
```

Pour plus d'informations sur l'utilisation de Lambda avec AWS IoT, consultez Création d'une AWS Lambda règle.

Utilisation de Lambda pour traiter les enregistrements à partir d'Amazon Kinesis Data Streams

Vous pouvez utiliser une fonction d'événement Lambda pour traiter les enregistrements d'un flux de données Amazon Kinesis. Vous pouvez associer une fonction d'événement Lambda à un client à débit partagé Kinesis Data Streams (itérateur standard) ou à un consommateur à débit dédié doté d'un ventilateur amélioré. Pour les itérateurs standard, Lambda interroge chaque partition de votre flux Kinesis pour des enregistrements qui utilisent le protocole HTTP. Le mappage de source d'événement partage le débit de lecture avec d'autres utilisateurs de la partition.

Pour plus d'informations sur les flux de données Kinesis, consultez Lecture de données à partir d'Amazon Kinesis Data Streams.

Consultez the section called "Créer un mappage" pour démarrer. Vous pouvez configurer les paramètres de mappage des sources d'événements, utiliser des fenêtres de défilement pour l'agrégation et consulter des exemples de code de fonction.

> **Note**
>
> Kinesis facture chaque partition et, pour les diffusions améliorées, les données lues à partir du flux. Pour obtenir des informations de tarification, consultez Tarification Amazon Kinesis.

Flux d'interrogation et de mise en lots

Lambda lit les enregistrements du flux de données et invoque votre fonction de manière synchrone avec un événement contenant des enregistrements de flux. Lambda lit les registres par lots et invoque votre fonction pour les traiter. Chaque lot contient des enregistrements provenant d'un seul shard/data flux.

Votre fonction d'événement Lambda est une application grand public pour votre flux de données. Elle traite un lot d'enregistrements à la fois à partir de chaque partition. Vous pouvez associer une fonction d'événement Lambda à un consommateur à débit partagé (itérateur standard) ou à un consommateur à débit dédié doté d'un ventilateur amélioré.

- Itérateur standard : Lambda interroge chaque partition de votre flux Kinesis afin d'obtenir des enregistrements à une fréquence de base d'une fois par seconde. Lorsque d'autres enregistrements sont disponibles, Lambda continue de traiter les lots jusqu'à ce que la fonction

rattrape le flux. Le mappage de source d'événement partage le débit de lecture avec d'autres utilisateurs de la partition.

- Diffusion améliorée : pour réduire la latence et optimiser le débit en lecture, créez un consommateur de flux de données avec diffusion améliorée. Les consommateurs avec diffusion améliorée obtiennent une connexion dédiée pour chaque partition qui n'a pas d'impact sur les autres applications lisant sur le flux. Les consommateurs de streaming ont l' HTTP/2 habitude de réduire le temps de latence en transférant les enregistrements vers Lambda via une connexion de longue durée et en compressant les en-têtes des demandes. Vous pouvez créer un consommateur de flux à l'aide de l'API Kinesis RegisterStreamConsumer.

```
aws kinesis register-stream-consumer \
--consumer-name con1 \
--stream-arn arn:aws:kinesis:us-east-2:123456789012:stream/lambda-stream
```

Vous devriez voir la sortie suivante :

```
{
    "Consumer": {
        "ConsumerName": "con1",
        "ConsumerARN": "arn:aws:kinesis:us-east-2:123456789012:stream/lambda-stream/
consumer/con1:1540591608",
        "ConsumerStatus": "CREATING",
        "ConsumerCreationTimestamp": 1540591608.0
    }
}
```

Pour augmenter la vitesse à laquelle votre fonction traite les enregistrements, ajoutez des partitions à votre flux de données. Lambda traite les enregistrements de chaque partition dans l'ordre. Il arrête de traiter les enregistrements supplémentaires d'une partition si votre fonction renvoie une erreur. Plus de partitions signifient plus de lots traités en une seule fois, ce qui réduit l'impact des erreurs sur la simultanéité.

Si votre fonction ne peut pas augmenter sa capacité pour traiter le nombre total de lots simultanés, demandez une augmentation de quota ou réservez de la simultanéité pour votre fonction.

Par défaut, Lambda invoque votre fonction dès que des enregistrements sont disponibles. Si le lot que Lambda lit à partir de la source d'événements ne comprend qu'un seul enregistrement, Lambda envoie un seul registre à la fonction. Pour éviter d'invoquer la fonction avec un petit nombre de registres, vous pouvez indiquer à la source d'événement de les mettre en mémoire tampon pendant

5 minutes en configurant une fenêtre de traitement par lots. Avant d'invoquer la fonction, Lambda continue de lire les registres de la source d'événements jusqu'à ce qu'il ait rassemblé un lot complet, que la fenêtre de traitement par lot expire ou que le lot atteigne la limite de charge utile de 6 Mo. Pour plus d'informations, consultez Comportement de traitement par lots.

> **Warning**
>
> Les mappages des sources d'événements Lambda traitent chaque événement au moins une fois, et le traitement des enregistrements peut être dupliqué. Pour éviter les problèmes potentiels liés à des événements dupliqués, nous vous recommandons vivement de rendre votre code de fonction idempotent. Pour en savoir plus, consultez Comment rendre ma fonction Lambda idempotente dans le Knowledge Center. AWS

Lambda envoi le prochain lot pour traitement sans attendre que les extensions configurées soient terminées. En d'autres termes, vos extensions peuvent continuer à s'exécuter pendant que Lambda traite le prochain lot d'enregistrements. Cela peut causer des problèmes de limitation si vous enfreignez l'un des paramètres ou l'une des limites de simultanéité de votre compte. Pour détecter s'il s'agit d'un problème éventuel, surveillez vos fonctions et vérifiez si vous observez des métriques de simultanéité plus élevées que prévu pour votre mappage des sources d'événements. En raison de la brièveté des intervalles entre les invocations, Lambda peut brièvement signaler une utilisation simultanée supérieure au nombre de partitions. Cela peut être vrai même pour les fonctions d'événement Lambda sans extensions.

Configurez le ParallelizationFactorparamètre pour traiter une partition d'un flux de données Kinesis avec plusieurs invocations Lambda simultanément. Vous pouvez spécifier le nombre de lots simultanés que Lambda interroge à partir d'une partition en utilisant un facteur de parallélisation compris entre 1 (par défaut) et 10. Par exemple, lorsque vous définissez la `ParallelizationFactor` valeur 2, vous pouvez avoir 200 appels Lambda simultanés au maximum pour traiter 100 fragments de données Kinesis (bien qu'en pratique, vous puissiez voir des valeurs différentes pour la métrique). `ConcurrentExecutions` Cela permet d'augmenter le débit de traitement quand le volume de données est volatil et que la valeur du paramètre `IteratorAge` est élevée. Lorsque vous augmentez le nombre de lots simultanés par partition, Lambda assure toujours un traitement dans l'ordre au niveau clé de partition.

Vous pouvez également utiliser `ParallelizationFactor` avec l'agrégation Kinesis. Le comportement du mappage des sources d'événements varie selon que vous utilisez ou non une diffusion améliorée :

- Sans diffusion améliorée : tous les événements d'un événement agrégé doivent avoir la même clé de partition. La clé de partition doit également correspondre à celle de l'événement agrégé. Si les événements contenus dans l'événement agrégé ont des clés de partition différentes, Lambda ne peut garantir le traitement dans l'ordre des événements par clé de partition.
- Avec une diffusion améliorée : Lambda décode d'abord l'événement agrégé en événements individuels. L'événement agrégé peut avoir une clé de partition différente de celle des événements qu'il contient. Cependant, les événements qui ne correspondent pas à la clé de partition sont supprimés et perdus. Lambda ne traite pas ces événements et ne les envoie pas vers une destination en cas de panne configurée.

Exemple d'évènement

Example

```
{
    "Records": [
        {
            "kinesis": {
                "kinesisSchemaVersion": "1.0",
                "partitionKey": "1",
                "sequenceNumber":
 "49590338271490256608559692538361571095921575989136588898",
                "data": "SGVsbG8sIHRoaXMgaXMgYSB0ZXN0Lg==",
                "approximateArrivalTimestamp": 1545084650.987
            },
            "eventSource": "aws:kinesis",
            "eventVersion": "1.0",
            "eventID":
 "shardId-000000000006:49590338271490256608559692538361571095921575989136588898",
            "eventName": "aws:kinesis:record",
            "invokeIdentityArn": "arn:aws:iam::123456789012:role/lambda-role",
            "awsRegion": "us-east-2",
            "eventSourceARN": "arn:aws:kinesis:us-east-2:123456789012:stream/lambda-
stream"
        },
        {
            "kinesis": {
                "kinesisSchemaVersion": "1.0",
                "partitionKey": "1",
                "sequenceNumber":
 "49590338271490256608559692540925702759324208523137515618",
```

```
                "data": "VGhpcyBpcyBvbmx5IGEgdGVzdC4=",
                "approximateArrivalTimestamp": 1545084711.166
            },
            "eventSource": "aws:kinesis",
            "eventVersion": "1.0",
            "eventID":
 "shardId-000000000006:49590338271490256608559692540925702759324208523137515618",
            "eventName": "aws:kinesis:record",
            "invokeIdentityArn": "arn:aws:iam::123456789012:role/lambda-role",
            "awsRegion": "us-east-2",
            "eventSourceARN": "arn:aws:kinesis:us-east-2:123456789012:stream/lambda-
stream"
        }
    ]
}
```

Traitement des enregistrements Amazon Kinesis Data Streams avec Lambda

Pour traiter les enregistrements Amazon Kinesis Data Streams avec Lambda, créez un mappage des sources d'événements Lambda. Vous pouvez associer une fonction d'événement Lambda à un itérateur standard ou à un consommateur de ventilateurs amélioré. Pour plus d'informations, consultez Flux d'interrogation et de mise en lots.

Créer un mappage des sources d'événements Kinesis

Pour appeler votre fonction d'événement Lambda avec les enregistrements de votre flux de données, créez un mappage des sources d'événements. Vous pouvez créer plusieurs mappages de sources d'événements pour traiter les mêmes données avec plusieurs fonctions d'événement Lambda, ou pour traiter des éléments provenant de plusieurs flux de données avec une seule fonction. Lorsque vous traitez des éléments à partir de plusieurs flux, chaque lot ne contient que des enregistrements provenant d'une seule partition ou d'un seul flux.

Vous pouvez configurer des mappages de sources d'événements pour traiter les enregistrements d'un flux dans un autre Compte AWS. Pour en savoir plus, consultez the section called "Cross-account mappages".

Avant de créer un mappage de source d'événements, vous devez autoriser votre fonction d'événement Lambda à lire un flux de données Kinesis. Lambda a besoin des autorisations suivantes pour gérer les ressources liées à votre flux de données Kinesis :

- kinésie : DescribeStream

- kinésie : DescribeStreamSummary
- kinésie : GetRecords
- kinésie : GetShardIterator
- kinésie : ListShards
- kinésie : SubscribeToShard

La politique AWS gérée AWSLambdaKinesisExecutionRoleinclut ces autorisations. Ajoutez cette politique gérée à votre fonction comme décrit dans la procédure suivante.

> **Note**
>
> - Vous n'avez pas besoin de l'autorisation `kinesis:ListStreams` pour créer et gérer des mappages des sources d'événements pour Kinesis. Toutefois, si vous créez un mappage des sources d'événements dans la console et que vous ne disposez pas de cette autorisation, vous ne pourrez pas sélectionner un flux Kinesis dans une liste déroulante et la console affichera un message d'erreur. Pour créer le mappage des sources d'événements, vous devez saisir manuellement l'Amazon Resource Name (ARN) de votre flux.
> - Lambda effectue des appels d'API `kinesis:GetRecords` et `kinesis:GetShardIterator` lorsqu'il tente à nouveau des appels qui ont échoué.

Console de gestion AWS

Pour ajouter des autorisations Kinesis à votre fonction événementielle

1. Ouvrez la page Event Functions de la console Lambda et sélectionnez votre fonction.
2. Sous l'onglet Configuration, sélectionnez Autorisations.
3. Dans le volet Rôle d'exécution, sous Nom du rôle, choisissez le lien vers le rôle d'exécution de votre fonction. Ce lien ouvre la page de ce rôle dans la console IAM.
4. Dans le volet Politiques d'autorisations, choisissez Ajouter des autorisations, puis sélectionnez Attacher des politiques.
5. Dans le champ de recherche, entrez **`AWSLambdaKinesisExecutionRole`**.
6. Cochez la case en regard de la politique, puis choisissez Ajouter une autorisation.

AWS CLI

Pour ajouter des autorisations Kinesis à votre fonction événementielle

- Exécutez la commande CLI suivante pour ajouter la `AWSLambdaKinesisExecutionRole` politique au rôle d'exécution de votre fonction :

```
aws iam attach-role-policy \
--role-name MyFunctionRole \
--policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaKinesisExecutionRole
```

AWS SAM

Pour ajouter des autorisations Kinesis à votre fonction événementielle

- Dans la définition de votre fonction, ajoutez la `Policies` propriété comme indiqué dans l'exemple suivant :

```
Resources:
  MyFunction:
    Type: AWS::Serverless::Function
    Properties:
      CodeUri: ./my-function/
      Handler: index.handler
      Runtime: nodejs24.x
      Policies:
        - AWSLambdaKinesisExecutionRole
```

Après avoir configuré les autorisations requises, créez le mappage des sources d'événements.

Console de gestion AWS

Pour créer le mappage des sources d'événements Kinesis

1. Ouvrez la page Event Functions de la console Lambda et sélectionnez votre fonction.
2. Dans le volet de Présentation de la fonction, choisissez Ajouter un déclencheur.
3. Sous Configuration du déclencheur, pour la source, sélectionnez Kinesis.
4. Sélectionnez le flux Kinesis pour lequel vous souhaitez créer le mappage des sources d'événements et, éventuellement, un consommateur de votre flux.

5. (Facultatif) Modifiez la Taille de lot, la Position de départ et la Fenêtre de traitement par lot de votre mappage des sources d'événements.
6. Choisissez Ajouter.

Lorsque vous créez le mappage de vos sources d'événements depuis la console, votre rôle IAM doit disposer des autorisations kinesis : ListStreams et kinesis :. ListStreamConsumers

AWS CLI

Pour créer le mappage des sources d'événements Kinesis

- Exécutez la commande de la CLI suivante pour créer un mappage des sources d'événements Kinesis. Choisissez votre propre taille de lot et votre position de départ en fonction de votre cas d'utilisation.

```
aws lambda create-event-source-mapping \
--function-name MyFunction \
--event-source-arn arn:aws:kinesis:us-east-2:123456789012:stream/lambda-stream \
--starting-position LATEST \
--batch-size 100
```

Pour spécifier une fenêtre de traitement par lot, ajoutez l'option `--maximum-batching-window-in-seconds`. Pour plus d'informations sur ce paramètre et d'autres, consultez create-event-source-mapping dans la Référence des commandes de l'AWS CLI .

AWS SAM

Pour créer le mappage des sources d'événements Kinesis

- Dans la définition de votre fonction, ajoutez la `KinesisEvent` propriété comme indiqué dans l'exemple suivant :

```
Resources:
  MyFunction:
    Type: AWS::Serverless::Function
    Properties:
      CodeUri: ./my-function/
      Handler: index.handler
      Runtime: nodejs24.x
      Policies:
```

```
        - AWSLambdaKinesisExecutionRole
      Events:
        KinesisEvent:
          Type: Kinesis
          Properties:
            Stream: !GetAtt MyKinesisStream.Arn
            StartingPosition: LATEST
            BatchSize: 100

  MyKinesisStream:
    Type: AWS::Kinesis::Stream
    Properties:
      ShardCount: 1
```

Pour en savoir plus sur la création d'un mappage des sources d'événements pour Kinesis Data Streams AWS SAM in, consultez Kinesis dans AWS Serverless Application Model le manuel du développeur.

Position de départ du sondage et du stream

Sachez que l'interrogation des flux lors des mises à jour et de la création du mappage des sources d'événements est finalement cohérente.

- Lors de la création du mappage des sources d'événements, le démarrage de l'interrogation des événements depuis le flux peut prendre plusieurs minutes.
- Lors des mises à jour du mappage des sources d'événements, l'arrêt et le redémarrage de l'interrogation des événements depuis le flux peuvent prendre plusieurs minutes.

Ce comportement signifie que si vous spécifiez `LATEST` comme position de départ du flux, le mappage des sources d'événements peut manquer des événements lors de la création ou des mises à jour. Pour vous assurer de ne manquer aucun événement, spécifiez la position de départ du flux comme `TRIM_HORIZON` ou `AT_TIMESTAMP`.

Création d'un mappage des sources d'événements entre comptes

Amazon Kinesis Data Streams prend en charge les politiques basées sur les ressources. De ce fait, vous pouvez traiter les données ingérées dans un flux en un Compte AWS avec une fonction d'événement Lambda dans un autre compte.

Pour créer un mappage de source d'événements pour votre fonction d'événement Lambda à l'aide d'un flux Kinesis dans un autre Compte AWS, vous devez configurer le flux à l'aide d'une politique basée sur les ressources afin d'autoriser votre fonction d'événement Lambda à lire des éléments. Pour savoir comment configurer votre stream afin d'autoriser l'accès entre comptes, consultez la section Partage de l'accès avec des AWS Lambda fonctions multicomptes dans le guide du développeur Amazon Kinesis Streams.

Une fois que vous avez configuré votre flux avec une politique basée sur les ressources qui donne à votre fonction d'événement Lambda les autorisations requises, créez le mappage des sources d'événements à l'aide de l'une des méthodes décrites dans la section précédente.

Si vous choisissez de créer votre mappage des sources d'événements à l'aide de la console Lambda, collez l'ARN de votre flux directement dans la zone de saisie. Si vous souhaitez spécifier un consommateur pour votre flux, le champ du flux est automatiquement rempli lorsque l'ARN du consommateur est collé.

Configuration d'une réponse par lots partielle avec Kinesis Data Streams et Lambda

Lors de l'utilisation et du traitement de données de streaming à partir d'une source d'événement, par défaut, Lambda n'effectue un point de contrôle sur le numéro de séquence le plus élevé d'un lot que lorsque celui-ci est un succès complet. Lambda traite tous les autres résultats comme un échec complet et recommence à traiter le lot jusqu'à atteindre la limite de nouvelles tentatives. Pour autoriser des succès partiels lors du traitement des lots à partir d'un flux, activez `ReportBatchItemFailures`. Autoriser les réussites partielles peut contribuer à réduire le nombre de tentatives sur un enregistrement, mais cela n'empêche pas totalement la possibilité de nouvelles tentatives dans un enregistrement réussi.

Pour activer `ReportBatchItemFailures`, incluez la valeur enum **`ReportBatchItemFailures`** dans la listeFunctionResponseTypes. Cette liste indique les types de réponse activés pour votre fonction événementielle. Vous pouvez configurer cette liste lorsque vous créez ou mettez à jour un mappage des sources d'événements.

> **Note**
>
> Même lorsque votre code de fonction renvoie des réponses partielles en cas d'échec par lots, ces réponses ne sont pas traitées par Lambda, sauf si la `ReportBatchItemFailures` fonctionnalité est explicitement activée pour le mappage de la source de votre événement.

Syntaxe du rapport

Lors de la configuration des rapports d'échec d'articles de lot, la classe `StreamsEventResponse` est renvoyée avec une liste d'échecs d'articles de lot. Vous pouvez utiliser un objet `StreamsEventResponse` pour renvoyer le numéro de séquence du premier enregistrement ayant échoué dans le lot. Vous pouvez également créer votre classe personnalisée en utilisant la syntaxe de réponse correcte. La structure JSON suivante montre la syntaxe de réponse requise :

```
{
  "batchItemFailures": [
        {
            "itemIdentifier": "<SequenceNumber>"
        }
    ]
}
```

> **Note**
>
> Si le tableau `batchItemFailures` contient plusieurs éléments, Lambda utilise l'enregistrement portant le numéro de séquence le plus bas comme point de contrôle. Lambda réessaie ensuite tous les enregistrements à partir de ce point de contrôle.

Conditions de réussite et d'échec

Lambda traite un lot comme un succès complet si vous renvoyez l'un des éléments suivants :

- Une liste `batchItemFailure` vide
- Une liste `batchItemFailure` nulle
- Une `EventResponse` vide
- Un nu `EventResponse`

Lambda traite un lot comme un échec complet si vous renvoyez l'un des éléments suivants :

- Une chaîne vid `itemIdentifier`
- Un `itemIdentifier` nul
- Un `itemIdentifier` avec un nom de clé incorrect

Lambda effectue des nouvelles tentatives en cas d'échec en fonction de votre stratégie de nouvelle tentative.

Diviser un lot

Si votre invocation échoue et que `BisectBatchOnFunctionError` est activé, le lot est divisé en deux quel que soit votre paramètre `ReportBatchItemFailures`.

Quand une réponse de succès partiel de lot est reçue et que les paramètres `BisectBatchOnFunctionError` et `ReportBatchItemFailures` sont activés, le lot est divisé au numéro de séquence renvoyé, et Lambda n'effectue de nouvelle tentative que sur les enregistrements restants.

Pour simplifier la mise en œuvre de la logique de réponse partielle par lots, pensez à utiliser l'utilitaire Batch Processor de Powertools for AWS Lambda, qui gère automatiquement ces complexités pour vous.

Voici quelques exemples de codes de fonctions qui renvoient la liste des identifiants des messages ayant échoué dans le lot :

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signalement des échecs d'articles par lots Kinesis avec Lambda à l'aide de .NET.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
using System.Text;
using System.Text.Json.Serialization;
using Amazon.Lambda.Core;
using Amazon.Lambda.KinesisEvents;
using AWS.Lambda.Powertools.Logging;

// Assembly attribute to enable the Lambda function's JSON input to be converted
 into a .NET class.
```

```
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSeri

namespace KinesisIntegration;

public class Function
{
    // Powertools Logger requires an environment variables against your function
    // POWERTOOLS_SERVICE_NAME
    [Logging(LogEvent = true)]
    public async Task<StreamsEventResponse> FunctionHandler(KinesisEvent evnt,
 ILambdaContext context)
    {
        if (evnt.Records.Count == 0)
        {
            Logger.LogInformation("Empty Kinesis Event received");
            return new StreamsEventResponse();
        }

        foreach (var record in evnt.Records)
        {
            try
            {
                Logger.LogInformation($"Processed Event with EventId:
 {record.EventId}");
                string data = await GetRecordDataAsync(record.Kinesis, context);
                Logger.LogInformation($"Data: {data}");
                // TODO: Do interesting work based on the new data
            }
            catch (Exception ex)
            {
                Logger.LogError($"An error occurred {ex.Message}");
                /* Since we are working with streams, we can return the failed
 item immediately.
                   Lambda will immediately begin to retry processing from this
 failed item onwards. */
                return new StreamsEventResponse
                {
                    BatchItemFailures = new
 List<StreamsEventResponse.BatchItemFailure>
                    {
                        new StreamsEventResponse.BatchItemFailure
 { ItemIdentifier = record.Kinesis.SequenceNumber }
                    }
```

```
                };
            }
        }
        Logger.LogInformation($"Successfully processed {evnt.Records.Count}
 records.");
        return new StreamsEventResponse();
    }

    private async Task<string> GetRecordDataAsync(KinesisEvent.Record record,
 ILambdaContext context)
    {
        byte[] bytes = record.Data.ToArray();
        string data = Encoding.UTF8.GetString(bytes);
        await Task.CompletedTask; //Placeholder for actual async work
        return data;
    }
}

public class StreamsEventResponse
{
    [JsonPropertyName("batchItemFailures")]
    public IList<BatchItemFailure> BatchItemFailures { get; set; }
    public class BatchItemFailure
    {
        [JsonPropertyName("itemIdentifier")]
        public string ItemIdentifier { get; set; }
    }
}
```

Go

Kit SDK pour Go V2

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signalement des échecs d'articles par lots Kinesis avec Lambda à l'aide de Go.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
```

```
// SPDX-License-Identifier: Apache-2.0
package main

import (
 "context"
 "fmt"
 "github.com/aws/aws-lambda-go/events"
 "github.com/aws/aws-lambda-go/lambda"
)

func handler(ctx context.Context, kinesisEvent events.KinesisEvent)
 (map[string]interface{}, error) {
 batchItemFailures := []map[string]interface{}{}

 for _, record := range kinesisEvent.Records {
  curRecordSequenceNumber := ""

  // Process your record
  if /* Your record processing condition here */ {
   curRecordSequenceNumber = record.Kinesis.SequenceNumber
  }

  // Add a condition to check if the record processing failed
  if curRecordSequenceNumber != "" {
   batchItemFailures = append(batchItemFailures, map[string]interface{}
{"itemIdentifier": curRecordSequenceNumber})
  }
 }

 kinesisBatchResponse := map[string]interface{}{
  "batchItemFailures": batchItemFailures,
 }
 return kinesisBatchResponse, nil
}

func main() {
 lambda.Start(handler)
}
```

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signalement des échecs d'articles par lots Kinesis avec Lambda à l'aide de Java.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.KinesisEvent;
import com.amazonaws.services.lambda.runtime.events.StreamsEventResponse;

import java.io.Serializable;
import java.util.ArrayList;
import java.util.List;

public class ProcessKinesisRecords implements RequestHandler<KinesisEvent,
 StreamsEventResponse> {

    @Override
    public StreamsEventResponse handleRequest(KinesisEvent input, Context
 context) {

        List<StreamsEventResponse.BatchItemFailure> batchItemFailures = new
 ArrayList<>();
        String curRecordSequenceNumber = "";

        for (KinesisEvent.KinesisEventRecord kinesisEventRecord :
 input.getRecords()) {
            try {
                //Process your record
                KinesisEvent.Record kinesisRecord =
 kinesisEventRecord.getKinesis();
                curRecordSequenceNumber = kinesisRecord.getSequenceNumber();

            } catch (Exception e) {
```

```
                /* Since we are working with streams, we can return the failed
 item immediately.
                   Lambda will immediately begin to retry processing from this
 failed item onwards. */
                batchItemFailures.add(new
 StreamsEventResponse.BatchItemFailure(curRecordSequenceNumber));
                return new StreamsEventResponse(batchItemFailures);
            }
        }

       return new StreamsEventResponse(batchItemFailures);
    }
}
```

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signalement des échecs d'articles par lots Kinesis avec Lambda à l'aide de JavaScript.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
exports.handler = async (event, context) => {
  for (const record of event.Records) {
    try {
      console.log(`Processed Kinesis Event - EventID: ${record.eventID}`);
      const recordData = await getRecordDataAsync(record.kinesis);
      console.log(`Record Data: ${recordData}`);
      // TODO: Do interesting work based on the new data
    } catch (err) {
      console.error(`An error occurred ${err}`);
      /* Since we are working with streams, we can return the failed item
 immediately.
           Lambda will immediately begin to retry processing from this failed
 item onwards. */
```

```
      return {
        batchItemFailures: [{ itemIdentifier: record.kinesis.sequenceNumber }],
      };
    }
  }
  console.log(`Successfully processed ${event.Records.length} records.`);
  return { batchItemFailures: [] };
};

async function getRecordDataAsync(payload) {
  var data = Buffer.from(payload.data, "base64").toString("utf-8");
  await Promise.resolve(1); //Placeholder for actual async work
  return data;
}
```

Signaler les défaillances d'éléments de lot Kinesis avec Lambda à l'aide de. TypeScript

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import {
  KinesisStreamEvent,
  Context,
  KinesisStreamHandler,
  KinesisStreamRecordPayload,
  KinesisStreamBatchResponse,
} from "aws-lambda";
import { Buffer } from "buffer";
import { Logger } from "@aws-lambda-powertools/logger";

const logger = new Logger({
  logLevel: "INFO",
  serviceName: "kinesis-stream-handler-sample",
});

export const functionHandler: KinesisStreamHandler = async (
  event: KinesisStreamEvent,
  context: Context
): Promise<KinesisStreamBatchResponse> => {
  for (const record of event.Records) {
    try {
      logger.info(`Processed Kinesis Event - EventID: ${record.eventID}`);
      const recordData = await getRecordDataAsync(record.kinesis);
```

```
      logger.info(`Record Data: ${recordData}`);
      // TODO: Do interesting work based on the new data
    } catch (err) {
      logger.error(`An error occurred ${err}`);
      /* Since we are working with streams, we can return the failed item
 immediately.
           Lambda will immediately begin to retry processing from this failed
 item onwards. */
      return {
        batchItemFailures: [{ itemIdentifier: record.kinesis.sequenceNumber }],
      };
    }
  }
  logger.info(`Successfully processed ${event.Records.length} records.`);
  return { batchItemFailures: [] };
};

async function getRecordDataAsync(
  payload: KinesisStreamRecordPayload
): Promise<string> {
  var data = Buffer.from(payload.data, "base64").toString("utf-8");
  await Promise.resolve(1); //Placeholder for actual async work
  return data;
}
```

PHP

Kit SDK pour PHP

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signalement des échecs d'articles par lots Kinesis avec Lambda à l'aide de PHP.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
<?php
```

```
# using bref/bref and bref/logger for simplicity

use Bref\Context\Context;
use Bref\Event\Kinesis\KinesisEvent;
use Bref\Event\Handler as StdHandler;
use Bref\Logger\StderrLogger;

require __DIR__ . '/vendor/autoload.php';

class Handler implements StdHandler
{
    private StderrLogger $logger;
    public function __construct(StderrLogger $logger)
    {
        $this->logger = $logger;
    }

    /**
     * @throws JsonException
     * @throws \Bref\Event\InvalidLambdaEvent
     */
    public function handle(mixed $event, Context $context): array
    {
        $kinesisEvent = new KinesisEvent($event);
        $this->logger->info("Processing records");
        $records = $kinesisEvent->getRecords();

        $failedRecords = [];
        foreach ($records as $record) {
            try {
                $data = $record->getData();
                $this->logger->info(json_encode($data));
                // TODO: Do interesting work based on the new data
            } catch (Exception $e) {
                $this->logger->error($e->getMessage());
                // failed processing the record
                $failedRecords[] = $record->getSequenceNumber();
            }
        }
        $totalRecords = count($records);
        $this->logger->info("Successfully processed $totalRecords records");

        // change format for the response
        $failures = array_map(
```

```
            fn(string $sequenceNumber) => ['itemIdentifier' => $sequenceNumber],
            $failedRecords
        );

        return [
            'batchItemFailures' => $failures
        ];
    }
}

$logger = new StderrLogger();
return new Handler($logger);
```

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signalement des échecs d'articles par lots Kinesis avec Lambda à l'aide de Python.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
def handler(event, context):
    records = event.get("Records")
    curRecordSequenceNumber = ""

    for record in records:
        try:
            # Process your record
            curRecordSequenceNumber = record["kinesis"]["sequenceNumber"]
        except Exception as e:
            # Return failed record's sequence number
            return {"batchItemFailures":[{"itemIdentifier":
 curRecordSequenceNumber}]}

    return {"batchItemFailures":[]}
```

Ruby

Kit SDK pour Ruby

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signalement des échecs d'articles par lots Kinesis avec Lambda à l'aide de Ruby.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
require 'aws-sdk'

def lambda_handler(event:, context:)
  batch_item_failures = []

  event['Records'].each do |record|
    begin
      puts "Processed Kinesis Event - EventID: #{record['eventID']}"
      record_data = get_record_data_async(record['kinesis'])
      puts "Record Data: #{record_data}"
      # TODO: Do interesting work based on the new data
    rescue StandardError => err
      puts "An error occurred #{err}"
      # Since we are working with streams, we can return the failed item
 immediately.
      # Lambda will immediately begin to retry processing from this failed item
 onwards.
      return { batchItemFailures: [{ itemIdentifier: record['kinesis']
['sequenceNumber'] }] }
    end
  end

  puts "Successfully processed #{event['Records'].length} records."
  { batchItemFailures: batch_item_failures }
end
```

```
def get_record_data_async(payload)
  data = Base64.decode64(payload['data']).force_encoding('utf-8')
  # Placeholder for actual async work
  sleep(1)
  data
end
```

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signalement des échecs d'articles par lots Kinesis avec Lambda à l'aide de Rust.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
use aws_lambda_events::{
    event::kinesis::KinesisEvent,
    kinesis::KinesisEventRecord,
    streams::{KinesisBatchItemFailure, KinesisEventResponse},
};
use lambda_runtime::{run, service_fn, Error, LambdaEvent};

async fn function_handler(event: LambdaEvent<KinesisEvent>) ->
 Result<KinesisEventResponse, Error> {
    let mut response = KinesisEventResponse {
        batch_item_failures: vec![],
    };

    if event.payload.records.is_empty() {
        tracing::info!("No records found. Exiting.");
        return Ok(response);
    }

    for record in &event.payload.records {
        tracing::info!(
            "EventId: {}",
```

```
            record.event_id.as_deref().unwrap_or_default()
        );

        let record_processing_result = process_record(record);

        if record_processing_result.is_err() {
            response.batch_item_failures.push(KinesisBatchItemFailure {
                item_identifier: record.kinesis.sequence_number.clone(),
            });
            /* Since we are working with streams, we can return the failed item
 immediately.
            Lambda will immediately begin to retry processing from this failed
 item onwards. */
            return Ok(response);
        }
    }

    tracing::info!(
        "Successfully processed {} records",
        event.payload.records.len()
    );

    Ok(response)
}

fn process_record(record: &KinesisEventRecord) -> Result<(), Error> {
    let record_data = std::str::from_utf8(record.kinesis.data.as_slice());

    if let Some(err) = record_data.err() {
        tracing::error!("Error: {}", err);
        return Err(Error::from(err));
    }

    let record_data = record_data.unwrap_or_default();

    // do something interesting with the data
    tracing::info!("Data: {}", record_data);

    Ok(())
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    tracing_subscriber::fmt()
```

```
        .with_max_level(tracing::Level::INFO)
        // disable printing the name of the module in every log line.
        .with_target(false)
        // disabling time is handy because CloudWatch will add the ingestion
 time.
        .without_time()
        .init();

    run(service_fn(function_handler)).await
}
```

Utilisation de Powertools pour AWS Lambda processeur par lots

L'utilitaire de traitement par lots de Powertools for gère AWS Lambda automatiquement la logique de réponse partielle par lots, réduisant ainsi la complexité de la mise en œuvre du signalement des défaillances par lots. Voici des exemples d'utilisation de l'utilitaire de traitement par lots :

Python

> **Note**
>
> Pour des exemples complets et des instructions de configuration, consultez la documentation de l'utilitaire de traitement par lots.

Traitement des enregistrements de flux Kinesis Data Streams à l'aide d' AWS Lambda un processeur par lots.

```
import json
from aws_lambda_powertools import Logger
from aws_lambda_powertools.utilities.batch import BatchProcessor, EventType,
 process_partial_response
from aws_lambda_powertools.utilities.data_classes import KinesisEvent
from aws_lambda_powertools.utilities.typing import LambdaContext

processor = BatchProcessor(event_type=EventType.KinesisDataStreams)
logger = Logger()

def record_handler(record):
    logger.info(record)
    # Your business logic here
```

```
    # Raise an exception to mark this record as failed

def lambda_handler(event, context: LambdaContext):
    return process_partial_response(
        event=event,
        record_handler=record_handler,
        processor=processor,
        context=context
    )
```

TypeScript

> **Note**
>
> Pour des exemples complets et des instructions de configuration, consultez la documentation de l'utilitaire de traitement par lots.

Traitement des enregistrements de flux Kinesis Data Streams à l'aide d' AWS Lambda un processeur par lots.

```
import { BatchProcessor, EventType, processPartialResponse } from '@aws-lambda-
powertools/batch';
import { Logger } from '@aws-lambda-powertools/logger';
import type { KinesisEvent, Context } from 'aws-lambda';

const processor = new BatchProcessor(EventType.KinesisDataStreams);
const logger = new Logger();

const recordHandler = async (record: any): Promise<void> => {
    logger.info('Processing record', { record });
    // Your business logic here
    // Throw an error to mark this record as failed
};

export const handler = async (event: KinesisEvent, context: Context) => {
    return processPartialResponse(event, recordHandler, processor, {
        context,
    });
};
```

Java

> **Note**
>
> Pour des exemples complets et des instructions de configuration, consultez la documentation de l'utilitaire de traitement par lots.

Traitement des enregistrements de flux Kinesis Data Streams à l'aide d' AWS Lambda un processeur par lots.

```
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.KinesisEvent;
import com.amazonaws.services.lambda.runtime.events.StreamsEventResponse;
import software.amazon.lambda.powertools.batch.BatchMessageHandlerBuilder;
import software.amazon.lambda.powertools.batch.handler.BatchMessageHandler;

public class KinesisStreamBatchHandler implements RequestHandler<KinesisEvent,
 StreamsEventResponse> {

    private final BatchMessageHandler<KinesisEvent, StreamsEventResponse> handler;

    public KinesisStreamBatchHandler() {
        handler = new BatchMessageHandlerBuilder()
                .withKinesisBatchHandler()
                .buildWithRawMessageHandler(this::processMessage);
    }

    @Override
    public StreamsEventResponse handleRequest(KinesisEvent kinesisEvent, Context
 context) {
        return handler.processBatch(kinesisEvent, context);
    }

    private void processMessage(KinesisEvent.KinesisEventRecord kinesisEventRecord,
 Context context) {
        // Process the stream record
    }
}
```

.NET

> **Note**
>
> Pour des exemples complets et des instructions de configuration, consultez la documentation de l'utilitaire de traitement par lots.

Traitement des enregistrements de flux Kinesis Data Streams à l'aide d' AWS Lambda un processeur par lots.

```
using System;
using System.Threading;
using System.Threading.Tasks;
using Amazon.Lambda.Core;
using Amazon.Lambda.KinesisEvents;
using Amazon.Lambda.Serialization.SystemTextJson;
using AWS.Lambda.Powertools.BatchProcessing;

[assembly: LambdaSerializer(typeof(DefaultLambdaJsonSerializer))]

namespace HelloWorld;

public class OrderEvent
{
    public string? OrderId { get; set; }
    public string? CustomerId { get; set; }
    public decimal Amount { get; set; }
    public DateTime OrderDate { get; set; }
}

internal class TypedKinesisRecordHandler : ITypedRecordHandler<OrderEvent>
{
    public async Task<RecordHandlerResult> HandleAsync(OrderEvent orderEvent,
 CancellationToken cancellationToken)
    {
        if (string.IsNullOrEmpty(orderEvent.OrderId))
        {
            throw new ArgumentException("Order ID is required");
        }

        return await Task.FromResult(RecordHandlerResult.None);
```

```
    }
}

public class Function
{
    [BatchProcessor(TypedRecordHandler = typeof(TypedKinesisRecordHandler))]
    public BatchItemFailuresResponse HandlerUsingTypedAttribute(KinesisEvent _)
    {
        return TypedKinesisStreamBatchProcessor.Result.BatchItemFailuresResponse;
    }
}
```

Retenir les enregistrements de lots supprimés pour une source d'événements de flux de données Kinesis dans Lambda

La gestion des erreurs pour les mappages de sources d'événements Kinesis dépend du fait que l'erreur se produit avant que la fonction d'événement ne soit invoquée ou pendant l'invocation de la fonction :

- Avant l'appel : si un mappage de source d'événement Lambda ne parvient pas à appeler la fonction en raison d'un ralentissement ou d'autres problèmes, il réessaie jusqu'à ce que les enregistrements expirent ou dépassent l'âge maximum configuré sur le mappage de source d'événement (). MaximumRecordAgeInSeconds
- Pendant l'appel : si la fonction est invoquée mais renvoie une erreur, Lambda réessaie jusqu'à ce que les enregistrements expirent, dépassent l'âge maximum MaximumRecordAgeInSeconds() ou atteignent le quota de nouvelles tentatives configuré (). MaximumRetryAttempts Pour les erreurs de fonctionnement, vous pouvez également configurer BisectBatchOnFunctionError, ce qui divise un lot défaillant en deux lots plus petits, isolant ainsi les mauvais enregistrements et évitant les délais d'attente. Le fractionnement des lots ne consomme pas le quota de nouvelles tentatives.

Si les mesures de gestion des erreurs échouent, Lambda ignore les enregistrements et poursuit le traitement des lots du flux. Avec les paramètres par défaut, cela signifie qu'un enregistrement défectueux peut bloquer le traitement sur la partition affectée pendant jusqu'à une semaine. Pour éviter cela, configurez le mappage de source d'événement de votre fonction avec un nombre raisonnable de nouvelles tentatives et un âge maximum d'enregistrement correspondant à votre cas d'utilisation.

Configuration des destinations pour les invocations ayant échoué

Pour conserver les enregistrements des appels de mappage des sources d'événements ayant échoué, ajoutez une destination au mappage des sources d'événements de votre fonction d'événement. Chaque enregistrement envoyé à la destination est un document JSON contenant les métadonnées sur l'invocation ayant échoué. Pour les destinations Amazon S3, Lambda envoie également l'intégralité de l'enregistrement d'invocation avec les métadonnées. Vous pouvez configurer n'importe quelle rubrique Amazon SNS, n'importe quelle file d'attente Amazon SQS, n'importe quel compartiment Amazon S3 ou Kafka comme destination.

Avec les destinations Amazon S3, vous pouvez utiliser la fonctionnalité Notifications d'événements Amazon S3 pour recevoir des notifications lorsque des objets sont chargés dans votre compartiment S3 de destination. Vous pouvez également configurer les notifications d'événements S3 pour appeler une autre fonction d'événement Lambda afin d'effectuer un traitement automatique des lots ayant échoué.

Votre rôle d'exécution doit disposer d'autorisations pour la destination :

- Pour une destination SQS : sqs : SendMessage
- Pour une destination SNS : SNS:Publish
- Pour une destination S3 : s3 : PutObject et s3 : ListBucket
- Pour une destination Kafka : kafka-cluster : WriteData

Vous pouvez configurer un sujet Kafka comme destination en cas d'échec pour vos mappages de sources d'événements Kafka. Lorsque Lambda ne parvient pas à traiter les enregistrements après avoir épuisé toutes les tentatives ou lorsque les enregistrements dépassent l'âge maximum, Lambda envoie les enregistrements ayant échoué à la rubrique Kafka spécifiée pour un traitement ultérieur. Reportez-vous à the section called "Destination de Kafka en cas d'échec".

Si vous avez activé le chiffrement avec votre propre clé KMS pour une destination S3, le rôle d'exécution de votre fonction doit également être autorisé à appeler kms : GenerateDataKey. Si la clé KMS et la destination du compartiment S3 se trouvent dans un compte différent de celui de votre fonction d'événement Lambda et de votre rôle d'exécution, configurez la clé KMS de manière à ce que le rôle d'exécution autorise les km :. GenerateDataKey

Pour configurer une destination en cas de panne à l'aide de la console, procédez comme suit :

1. Ouvrez la page Event Functions de la console Lambda.

2. Choisissez une fonction.
3. Sous Function overview (Vue d'ensemble de la fonction), choisissez Add destination (Ajouter une destination).
4. Pour Source, choisissez Invocation du mappage des sources d'événements.
5. Pour le mappage des sources d'événements, choisissez une source d'événements configurée pour cette fonction.
6. Pour Condition, sélectionnez En cas d'échec. Pour les invocations de mappage des sources d'événements, il s'agit de la seule condition acceptée.
7. Pour Type de destination, choisissez le type de destination auquel Lambda envoie les enregistrements d'invocation.
8. Pour Destination, choisissez une ressource.
9. Cliquez sur Enregistrer.

Vous pouvez également configurer une destination en cas de panne à l'aide de AWS Command Line Interface (AWS CLI). Par exemple, la commande create-event-source-mapping suivante ajoute un mappage des sources d'événements avec une destination SQS en cas d'échec à `MyFunction` :

```
aws lambda create-event-source-mapping \
--function-name "MyFunction" \
--event-source-arn arn:aws:kinesis:us-east-2:123456789012:stream/lambda-stream \
--destination-config '{"OnFailure": {"Destination": "arn:aws:sqs:us-
east-1:123456789012:dest-queue"}}'
```

La commande update-event-source-mapping suivante met à jour un mappage des sources d'événements pour envoyer les enregistrements d'invocation ayant échoué à une destination SNS après deux nouvelles tentatives, ou si les enregistrements datent de plus d'une heure.

```
aws lambda update-event-source-mapping \
--uuid f89f8514-cdd9-4602-9e1f-01a5b77d449b \
--maximum-retry-attempts 2 \
--maximum-record-age-in-seconds 3600 \
--destination-config '{"OnFailure": {"Destination": "arn:aws:sns:us-
east-1:123456789012:dest-topic"}}'
```

Les paramètres mis à jour sont appliqués de façon asynchrone et ne sont pas reflétés dans la sortie tant que le processus n'est pas terminé. Utilisez la commande get-event-source-mapping pour afficher l'état actuel.

Pour supprimer une destination, entrez une chaîne vide comme argument du paramètre `destination-config` :

```
aws lambda update-event-source-mapping \
--uuid f89f8514-cdd9-4602-9e1f-01a5b77d449b \
--destination-config '{"OnFailure": {"Destination": ""}}'
```

Pratiques exemplaires en matière de sécurité pour les destinations Amazon S3

La suppression d'un compartiment S3 configuré comme destination sans supprimer la destination de la configuration de votre fonction peut engendrer un risque de sécurité. Si un autre utilisateur connaît le nom de votre compartiment de destination, il peut recréer le compartiment dans son Compte AWS. Les enregistrements des invocations ayant échoué seront envoyés dans son compartiment, exposant potentiellement les données de votre fonction.

> **Warning**
>
> Pour vous assurer que les enregistrements d'invocation de votre fonction d'événement ne peuvent pas être envoyés vers un compartiment S3 d'un autre Compte AWS, ajoutez une condition au rôle d'exécution de votre fonction qui limite `s3:PutObject` les autorisations aux compartiments de votre compte.

L'exemple suivant présente une politique IAM qui limite les autorisations `s3:PutObject` de votre fonction aux seuls compartiments de votre compte. Cette politique donne également à Lambda l'autorisation `s3:ListBucket` dont il a besoin pour utiliser un compartiment S3 comme destination.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3BucketResourceAccountWrite",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::*/*",
                "arn:aws:s3:::*"
            ],
```

```
            "Condition": {
                "StringEquals": {
                    "s3:ResourceAccount": "111122223333"
                }
            }
        }
    ]
}
```

Pour ajouter une politique d'autorisations au rôle d'exécution de votre fonction à l'aide du Console de gestion AWS ou AWS CLI, reportez-vous aux instructions des procédures suivantes :

Console

Pour ajouter une politique d’autorisations au rôle d’exécution d’une fonction (console)

1. Ouvrez la page Event Functions de la console Lambda.
2. Sélectionnez la fonction d'événement Lambda dont vous souhaitez modifier le rôle d'exécution.
3. Sous l’onglet Configuration, sélectionnez Autorisations.
4. Sous l’onglet Rôle d’exécution, sélectionnez le Nom du rôle de votre fonction pour ouvrir la page de console IAM du rôle.
5. Ajoutez une politique d’autorisations de au rôle en procédant comme suit :
    a. Dans le volet Politiques d’autorisations, choisissez Ajouter des autorisations, puis Créer une politique en ligne.
    b. Dans l’Éditeur de politique, sélectionnez JSON.
    c. Collez la politique que vous souhaitez ajouter dans l’éditeur (en remplacement du JSON existant), puis choisissez Suivant.
    d. Sous Détails de la politique, saisissez un Nom de la politique.
    e. Choisissez Create Policy (Créer une politique).

AWS CLI

Pour ajouter une politique d'autorisation au rôle d'exécution (CLI) d'une fonction d'événement

1. Créez un document de politique JSON avec les autorisations requises et enregistrez-le dans un répertoire local.

2. Utilisez la commande `put-role-policy` de la CLI IAM pour ajouter des autorisations au rôle d'exécution de votre fonction. Exécutez la commande suivante depuis le répertoire dans lequel vous avez enregistré votre document de politique JSON et remplacez le nom du rôle, le nom de la politique et le document de politique par vos propres valeurs.

```
aws iam put-role-policy \
--role-name my_lambda_role \
--policy-name LambdaS3DestinationPolicy \
--policy-document file://my_policy.json
```

Exemple d'enregistrement d'invocation Amazon SNS et Amazon SQS

L'exemple suivant montre ce que Lambda envoie à une file d'attente SQS ou à une rubrique SNS en cas d'échec de l'invocation d'une source d'événement Kinesis. Étant donné que Lambda envoie uniquement les métadonnées pour ces types de destination, utilisez les champs `streamArn`, `shardId`, `startSequenceNumber` et `endSequenceNumber` pour obtenir l'enregistrement original complet. Tous les champs présentés dans la propriété `KinesisBatchInfo` seront toujours présents.

```
{
    "requestContext": {
        "requestId": "c9b8fa9f-5a7f-xmpl-af9c-0c604cde93a5",
        "functionArn": "arn:aws:lambda:us-east-2:123456789012:function:myfunction",
        "condition": "RetryAttemptsExhausted",
        "approximateInvokeCount": 1
    },
    "responseContext": {
        "statusCode": 200,
        "executedVersion": "$LATEST",
        "functionError": "Unhandled"
    },
    "version": "1.0",
    "timestamp": "2019-11-14T00:38:06.021Z",
    "KinesisBatchInfo": {
        "shardId": "shardId-000000000001",
        "startSequenceNumber":
 "49601189658422359378836298521827638475320189012309704722",
        "endSequenceNumber":
 "49601189658422359378836298522902373528957594348623495186",
        "approximateArrivalOfFirstRecord": "2019-11-14T00:38:04.835Z",
        "approximateArrivalOfLastRecord": "2019-11-14T00:38:05.580Z",
```

```
        "batchSize": 500,
        "streamArn": "arn:aws:kinesis:us-east-2:123456789012:stream/mystream"
    }
}
```

Vous pouvez utiliser ces informations pour récupérer les enregistrements concernés à partir du flux à des fins de résolution de problèmes. Les enregistrements réels n'étant pas inclus, vous devez les récupérer du flux avant qu'ils expirent et soient perdus.

Exemple d'enregistrement d'invocation Amazon S3

L'exemple suivant montre ce que Lambda envoie à un compartiment Amazon S3 ou à une invocation de source d'événement Kinesis. Outre tous les champs de l'exemple précédent pour les destinations SQS et SNS, le champ `payload` contient l'enregistrement d'invocation d'origine sous forme de chaîne JSON échappée.

```
{
    "requestContext": {
        "requestId": "c9b8fa9f-5a7f-xmpl-af9c-0c604cde93a5",
        "functionArn": "arn:aws:lambda:us-east-2:123456789012:function:myfunction",
        "condition": "RetryAttemptsExhausted",
        "approximateInvokeCount": 1
    },
    "responseContext": {
        "statusCode": 200,
        "executedVersion": "$LATEST",
        "functionError": "Unhandled"
    },
    "version": "1.0",
    "timestamp": "2019-11-14T00:38:06.021Z",
    "KinesisBatchInfo": {
        "shardId": "shardId-000000000001",
        "startSequenceNumber":
 "49601189658422359378836298521827638475320189012309704722",
        "endSequenceNumber":
 "49601189658422359378836298522902373528957594348623495186",
        "approximateArrivalOfFirstRecord": "2019-11-14T00:38:04.835Z",
        "approximateArrivalOfLastRecord": "2019-11-14T00:38:05.580Z",
        "batchSize": 500,
        "streamArn": "arn:aws:kinesis:us-east-2:123456789012:stream/mystream"
    },
    "payload": "<Whole Event>" // Only available in S3
```

```
}
```

L’objet S3 contenant l’enregistrement d’invocation utilise la convention de dénomination suivante :

```
aws/lambda/<ESM-UUID>/<shardID>/YYYY/MM/DD/YYYY-MM-DDTHH.MM.SS-<Random UUID>
```

Implémentation du traitement des flux de données Kinesis avec état dans Lambda

Les fonctions d'événement Lambda peuvent exécuter des applications de traitement de flux continu. Un flux représente des données illimitées qui circulent en continu dans votre application. Pour analyser les informations provenant de cette entrée de mise à jour continue, vous pouvez lier les enregistrements inclus à l’aide d’une fenêtre de temps définie.

Les fenêtres bascules sont des fenêtres temporelles distinctes qui s’ouvrent et se ferment à intervalles réguliers. Par défaut, les invocations Lambda sont sans état : vous ne pouvez pas les utiliser pour traiter des données sur plusieurs invocations continues sans base de données externe. Cependant, avec les fenêtres bascules, vous pouvez maintenir votre état au long des invocations.

Cet état contient le résultat global des messages précédemment traités pour la fenêtre actuelle. Votre état peut atteindre un maximum de 1 Mo pour chaque partition. S’il dépasse cette taille, Lambda met fin précocement à la fenêtre de traitement.

Chaque enregistrement d’un flux appartient à une fenêtre spécifique. Lambda traite chaque enregistrement au moins une fois, mais ne garantit pas que chaque enregistrement ne soit traité qu'une seule fois. Dans de rares cas, tels que pour la gestion des erreurs, certains enregistrements peuvent être sujet à de multiples traitements. Les dossiers sont toujours traités dans l’ordre dès la première fois. Si les enregistrements sont traités plusieurs fois, ils peuvent être traités dans le désordre.

Regroupement et traitement

Votre fonction gérée par l’utilisateur est invoquée tant pour l’agrégation que pour le traitement des résultats finaux de celle-ci. Lambda regroupe tous les enregistrements reçus dans la fenêtre. Vous pouvez recevoir ces enregistrements en plusieurs lots, chacun sous forme d’invocation séparée. Chaque invocation reçoit un état.

Ainsi, lorsque vous utilisez des fenêtres coulissantes, la réponse de votre fonction d'événement Lambda doit contenir `state` une propriété. Si la réponse ne contient pas de propriété `state`,

Lambda considère qu'il s'agit d'une invocation ayant échoué. Pour satisfaire à cette condition, votre fonction peut renvoyer un objet `TimeWindowEventResponse` ayant la forme JSON suivante :

Example **`TimeWindowEventResponse`** values

```
{
    "state": {
        "1": 282,
        "2": 715
    },
    "batchItemFailures": []
}
```

> **Note**
>
> Pour les fonctions Java, nous vous recommandons d'utiliser `Map<String, String>` pour représenter l'état.

À la fin de la fenêtre, l'indicateur `isFinalInvokeForWindow` est configuré `true` pour indiquer qu'il s'agit de l'état final et qu'il est prêt à être traité. Après le traitement, la fenêtre et votre invocation final se terminent, puis l'état est supprimé.

À la fin de votre fenêtre, Lambda applique un traitement final pour les actions sur les résultats de l'agrégation. Votre traitement final est invoqué de manière synchrone. Une fois l'invocation réussie, votre fonction contrôle le numéro de séquence et le traitement du flux continue. Si l'invocation échoue, votre fonction d'événement Lambda suspend le traitement ultérieur jusqu'à ce que l'appel aboutisse.

Example KinesisTimeWindowEvent

```
{
    "Records": [
        {
            "kinesis": {
                "kinesisSchemaVersion": "1.0",
                "partitionKey": "1",
                "sequenceNumber":
 "49590338271490256608559692538361571095921575989136588898",
```

```
                "data": "SGVsbG8sIHRoaXMgaXMgYSB0ZXN0Lg==",
                "approximateArrivalTimestamp": 1607497475.000
            },
            "eventSource": "aws:kinesis",
            "eventVersion": "1.0",
            "eventID":
 "shardId-000000000006:49590338271490256608559692538361571095921575989136588898",
            "eventName": "aws:kinesis:record",
            "invokeIdentityArn": "arn:aws:iam::123456789012:role/lambda-kinesis-role",
            "awsRegion": "us-east-1",
            "eventSourceARN": "arn:aws:kinesis:us-east-1:123456789012:stream/lambda-
stream"
        }
    ],
    "window": {
        "start": "2020-12-09T07:04:00Z",
        "end": "2020-12-09T07:06:00Z"
    },
    "state": {
        "1": 282,
        "2": 715
    },
    "shardId": "shardId-000000000006",
    "eventSourceARN": "arn:aws:kinesis:us-east-1:123456789012:stream/lambda-stream",
    "isFinalInvokeForWindow": false,
    "isWindowTerminatedEarly": false
}
```

Configuration

Vous pouvez configurer des fenêtres bascule lorsque vous créez ou mettez à jour un mappage de source d'événement. Pour configurer une fenêtre variable, spécifiez la fenêtre en secondes (TumblingWindowInSeconds). L'exemple de commande suivant AWS Command Line Interface (AWS CLI) crée un mappage des sources d'événements de streaming dont la fenêtre de basculement est de 120 secondes. La fonction d'événement Lambda définie pour l'agrégation et le traitement est nommée. `tumbling-window-example-function`

```
aws lambda create-event-source-mapping \
--event-source-arn arn:aws:kinesis:us-east-1:123456789012:stream/lambda-stream \
--function-name tumbling-window-example-function \
--starting-position TRIM_HORIZON \
--tumbling-window-in-seconds 120
```

Lambda détermine les limites des fenêtres bascule en fonction de l'heure à laquelle les enregistrements ont été insérés dans le flux. Tous les enregistrements ont un horodatage approximatif disponible que Lambda utilise pour déterminer des limites.

Les agrégations de fenêtres bascule ne prennent pas en charge le repartitionnement. Lorsqu'une partition se termine, Lambda considère que la fenêtre en cours est fermée, et toute partition enfant ouvre sa propre fenêtre dans un nouvel état. Lorsqu'aucun nouvel enregistrement n'est ajouté à la fenêtre actuelle, Lambda attend jusqu'à 2 minutes avant de supposer que la fenêtre est terminée. Cela permet de garantir que la fonction lit tous les enregistrements de la fenêtre actuelle, même si les enregistrements sont ajoutés par intermittence.

Les fenêtres bascule prennent complètement en charge les stratégies de nouvelle tentative existantes `maxRetryAttempts` et `maxRecordAge`.

Example Handler.py — Agrégation et traitement

La fonction Python suivante montre comment regrouper et traiter votre état final :

```
def lambda_handler(event, context):
    print('Incoming event: ', event)
    print('Incoming state: ', event['state'])

#Check if this is the end of the window to either aggregate or process.
    if event['isFinalInvokeForWindow']:
        # logic to handle final state of the window
        print('Destination invoke')
    else:
        print('Aggregate invoke')

#Check for early terminations
    if event['isWindowTerminatedEarly']:
        print('Window terminated early')

    #Aggregation logic
    state = event['state']
    for record in event['Records']:
        state[record['kinesis']['partitionKey']] = state.get(record['kinesis']
['partitionKey'], 0) + 1

    print('Returning state: ', state)
    return {'state': state}
```

Paramètres Lambda pour les mappages des sources d’événements Amazon Kinesis Data Streams

Tous les mappages de sources d'événements Lambda partagent les mêmes opérations CreateEventSourceMappinget UpdateEventSourceMappingles mêmes opérations d'API. Cependant, seuls certains paramètres s’appliquent à Kinesis.

Paramètre	Obligatoire	Par défaut	Remarques
BatchSize	N	100	Maximum : 10 000.
BisectBatchOnFunctionError	N	FAUX	Aucune
DestinationConfig	N	N/A	File d’attente Amazon SQS ou destination de rubrique Amazon SNS pour les enregistrements supprimés. Pour plus d’informations, consultez Configuration des destinations pour les invocations ayant échoué.
Enabled	N	VRAI	Aucune
EventSourceArn	Y	N/A	ARN du flux de données ou d’un consommateur de flux
FunctionName	O	N/A	Aucune
FunctionResponseTypes	N	N/A	Pour permettre à votre fonction événementielle de signaler des défaillances spécifiques dans

Paramètre	Obligatoire	Par défaut	Remarques
			un lot, incluez la valeur `ReportBatchItemFailures` dans `FunctionResponseTypes` . Pour plus d'informations, consultez Configuration d'une réponse par lots partielle avec Kinesis Data Streams et Lambda.
MaximumBatchingWindowInSeconds	N	0	Aucune
MaximumRecordAgeInSeconds	N	-1	-1 signifie infini : Lambda ne supprime pas les enregistrements (les paramètres de conservation des données Kinesis Data Streams s'appliquent toujours) Minimum : -1 Maximum : 604 800

Paramètre	Obligatoire	Par défaut	Remarques
MaximumRetryAttempts	N	-1	-1 signifie infini : les registres qui ont échoué sont réessayés jusqu'à ce que le registre expire. Minimum : -1 Maximum : 10 000.
ParallelizationFactor	N	1	Maximum : 10
StartingPosition	O	N/A	AT_TIMESTAMP, TRIM_HORIZON ou DERNIER
StartingPositionTimestamp	N	N/A	Valable uniquement s'il StartingPosition est défini sur AT_TIMESTAMP. L'heure à partir de laquelle commencer la lecture, en secondes au format horaire Unix.
TumblingWindowInSeconds	N	N/A	Minimum : 0 Maximum : 900

Utilisation du filtrage des événements avec une source d'événement Kinesis

Vous pouvez utiliser le filtrage des événements pour contrôler les enregistrements d'un flux ou d'une file d'attente que Lambda envoie à votre fonction d'événement. Pour obtenir des informations générales sur le fonctionnement du filtrage des événements, consultez the section called "Filtrage des événements".

Cette section porte sur le filtrage des événements pour les sources Kinesis.

> **Note**
>
> Les mappages des sources d'événements Kinesis prennent uniquement en charge le filtrage sur la clé `data`.

Rubriques

- Notions de base du filtrage des événements Kinesis
- Filtrage des enregistrements agrégés de Kinesis

Notions de base du filtrage des événements Kinesis

Supposons qu'un producteur insère des données au format JSON dans votre flux de données Kinesis. Un exemple d'enregistrement ressemblerait à ce qui suit, avec les données JSON converties en chaîne encodée en Base64 dans le champ `data`.

```
{
    "kinesis": {
        "kinesisSchemaVersion": "1.0",
        "partitionKey": "1",
        "sequenceNumber": "49590338271490256608559692538361571095921575989136588898",
        "data":
 "eyJSZWNvcmROdW1iZXIiOiAiMDAwMSIsICJUaW1lU3RhbXAiOiAieXl5eS1tbS1kZFRoaDptbTpzcyIsICJSZXF1ZXN0Q
        "approximateArrivalTimestamp": 1545084650.987
        },
    "eventSource": "aws:kinesis",
    "eventVersion": "1.0",
    "eventID":
 "shardId-000000000006:49590338271490256608559692538361571095921575989136588898",
    "eventName": "aws:kinesis:record",
    "invokeIdentityArn": "arn:aws:iam::123456789012:role/lambda-role",
    "awsRegion": "us-east-2",
    "eventSourceARN": "arn:aws:kinesis:us-east-2:123456789012:stream/lambda-stream"
}
```

Tant que les données insérées dans le flux par le producteur sont des données JSON valides, vous pouvez utiliser le filtrage d'événements pour filtrer les enregistrements à l'aide de la clé `data`.

Supposons qu'un producteur insère des enregistrements dans votre flux Kinesis au format JSON suivant.

```
{
    "record": 12345,
    "order": {
        "type": "buy",
        "stock": "ANYCO",
        "quantity": 1000
        }
}
```

Pour filtrer uniquement les enregistrements dont le type d'ordre est « achat », l'`FilterCriteria`objet serait le suivant.

```
{
    "Filters": [
        {
            "Pattern": "{ \"data\" : { \"order\" : { \"type\" : [ \"buy\" ] } } }"
        }
    ]
}
```

Pour plus de clarté, voici la valeur du `Pattern` de filtre étendu en JSON simple :

```
{
    "data": {
        "order": {
            "type": [ "buy" ]
            }
      }
}
```

Vous pouvez ajouter votre filtre à l'aide de la console AWS CLI ou d'un AWS SAM modèle.

Console

Pour ajouter ce filtre à l'aide de la console, suivez les instructions de Attacher des critères de filtre à un mappage de sources d'événements (console) et saisissez la chaîne suivante comme critère de filtre.

```
{ "data" : { "order" : { "type" : [ "buy" ] } } }
```

AWS CLI

Pour créer un nouveau mappage de source d'événements avec ces critères de filtre à l'aide de AWS Command Line Interface (AWS CLI), exécutez la commande suivante.

```
aws lambda create-event-source-mapping \
    --function-name my-function \
    --event-source-arn arn:aws:kinesis:us-east-2:123456789012:stream/my-stream \
    --filter-criteria '{"Filters": [{"Pattern": "{ \"data\" : { \"order\" : { \"type
\" : [ \"buy\" ] } } }"}]}'
```

Pour ajouter ces critères de filtre à un mappage des sources d'événements existant, exécutez la commande suivante.

```
aws lambda update-event-source-mapping \
    --uuid "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE" \
    --filter-criteria '{"Filters": [{"Pattern": "{ \"data\" : { \"order\" : { \"type
\" : [ \"buy\" ] } } }"}]}'
```

AWS SAM

Pour ajouter ce filtre AWS SAM, ajoutez l'extrait suivant au modèle YAML de votre source d'événement.

```
FilterCriteria:
  Filters:
    - Pattern: '{ "data" : { "order" : { "type" : [ "buy" ] } } }'
```

Pour filtrer correctement les événements provenant de sources Kinesis, le champ de données et vos critères de filtre pour le champ de données doivent être au format JSON valide. Si l'un ou l'autre des champs n'est pas dans un format JSON valide, Lambda rejette le message ou lance une exception. Le tableau suivant résume le comportement spécifique :

Format des données entrantes	Pas de modèle de filtre pour les propriétés des données	Action obtenue.
JSON valide	JSON valide	Lambda filtre en fonction de vos critères de filtre.
JSON valide	Pas de modèle de filtre pour les propriétés des données	Lambda filtre (uniquement selon les autres propriétés de métadonnées) en fonction de vos critères de filtre.
JSON valide	Non-JSON	Lambda lance une exception au moment de la création ou de la mise à jour du mappage de sources d'événements. Le modèle de filtre des propriétés de données doit être au format JSON valide.
Non-JSON	JSON valide	Lambda rejette l'enregis trement.
Non-JSON	Pas de modèle de filtre pour les propriétés des données	Lambda filtre (uniquement selon les autres propriétés de métadonnées) en fonction de vos critères de filtre.
Non-JSON	Non-JSON	Lambda lance une exception au moment de la création ou de la mise à jour du mappage de sources d'événements. Le modèle de filtre des propriétés de données doit être au format JSON valide.

Filtrage des enregistrements agrégés de Kinesis

Avec Kinesis, vous pouvez agréger plusieurs enregistrements en un seul enregistrement Kinesis Data Streams pour augmenter le débit de vos données. Lambda ne peut appliquer des critères de filtrage aux enregistrements agrégés que lorsque vous utilisez la distribution ramifiée améliorée de Kinesis. Le filtrage des enregistrements agrégés avec Kinesis standard n'est pas pris en charge. Lorsque vous utilisez un ventilateur amélioré, vous configurez un consommateur de débit dédié Kinesis pour qu'il déclenche votre fonction d'événement Lambda. Lambda filtre alors les enregistrements agrégés et ne transmet que les enregistrements qui répondent à vos critères de filtrage.

Pour en savoir plus sur l'agrégation d'enregistrements Kinesis, reportez-vous à la section Agrégation sur la page Concepts clés de Kinesis Producer Library (KPL). Pour en savoir plus sur l'utilisation de Lambda avec la fonction de ventilation améliorée de Kinesis, consultez la section Augmenter les performances de traitement des flux en temps réel grâce à la fonction de ventilation améliorée Amazon Kinesis Data Streams et à Lambda sur le blog consacré au calcul. AWS AWS

Tutoriel : Utilisation de Lambda avec les flux de données Kinesis

Dans ce didacticiel, vous allez créer une fonction d'événement Lambda pour utiliser les événements d'un flux de données Amazon Kinesis.

1. L'application personnalisée écrit les enregistrements dans le flux.
2. AWS Lambda interroge le flux et, lorsqu'il détecte de nouveaux enregistrements dans le flux, invoque votre fonction d'événement Lambda.
3. AWS Lambda exécute la fonction d'événement Lambda en assumant le rôle d'exécution que vous avez spécifié au moment de la création de la fonction d'événement Lambda.

Conditions préalables

Installer la AWS Command Line Interface

Si vous ne l'avez pas encore installé AWS Command Line Interface, suivez les étapes décrites dans la section Installation ou mise à jour de la dernière version du AWS CLI pour l'installer.

Ce tutoriel nécessite un terminal de ligne de commande ou un shell pour exécuter les commandes. Sous Linux et macOS, utilisez votre gestionnaire de shell et de package préféré.

> **Note**
>
> Sous Windows, certaines commandes CLI Bash que vous utilisez couramment avec Lambda (par exemple `zip`) ne sont pas prises en charge par les terminaux intégrés du système d'exploitation. Pour obtenir une Windows-integrated version d'Ubuntu et de Bash, installez le sous-système Windows pour Linux.

Créer le rôle d'exécution

Créez le rôle d'exécution qui autorise votre fonction à accéder aux AWS ressources.

Pour créer un rôle d'exécution

1. Ouvrez la page Roles (Rôles) dans la console IAM.
2. Sélectionnez Créer un rôle.
3. Créez un rôle avec les propriétés suivantes :
   - Entité de confiance – AWS Lambda.
   - Autorisations — AWSLambdaKinesisExecutionRole.
   - Nom de rôle – **`lambda-kinesis-role`**.

La AWSLambdaKinesisExecutionRolepolitique dispose des autorisations dont la fonction a besoin pour lire des éléments provenant de Kinesis et écrire des journaux dans Logs. CloudWatch

Création de la fonction d'événement

Créez une fonction d'événement Lambda qui traite vos messages Kinesis. Le code de fonction enregistre l'ID d'événement et les données d'événement de l'enregistrement Kinesis dans Logs. CloudWatch

Ce didacticiel utilise le runtime Node.js 24, mais nous avons également fourni des exemples de code dans d'autres langages d'exécution. Vous pouvez sélectionner l'onglet dans la zone suivante pour voir le code de l'exécution qui vous intéresse. Le JavaScript code que vous allez utiliser dans cette étape se trouve dans le premier exemple présenté dans l'JavaScriptonglet.

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement Kinesis avec Lambda à l'aide de .NET.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
using System.Text;
using Amazon.Lambda.Core;
using Amazon.Lambda.KinesisEvents;
using AWS.Lambda.Powertools.Logging;

// Assembly attribute to enable the Lambda function's JSON input to be converted
 into a .NET class.
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSeri

namespace KinesisIntegrationSampleCode;

public class Function
{
    // Powertools Logger requires an environment variables against your function
    // POWERTOOLS_SERVICE_NAME
    [Logging(LogEvent = true)]
    public async Task FunctionHandler(KinesisEvent evnt, ILambdaContext context)
    {
        if (evnt.Records.Count == 0)
        {
            Logger.LogInformation("Empty Kinesis Event received");
            return;
        }

        foreach (var record in evnt.Records)
        {
            try
            {
```

```
                Logger.LogInformation($"Processed Event with EventId:
 {record.EventId}");
                string data = await GetRecordDataAsync(record.Kinesis, context);
                Logger.LogInformation($"Data: {data}");
                // TODO: Do interesting work based on the new data
            }
            catch (Exception ex)
            {
                Logger.LogError($"An error occurred {ex.Message}");
                throw;
            }
        }
        Logger.LogInformation($"Successfully processed {evnt.Records.Count}
 records.");
    }

    private async Task<string> GetRecordDataAsync(KinesisEvent.Record record,
 ILambdaContext context)
    {
        byte[] bytes = record.Data.ToArray();
        string data = Encoding.UTF8.GetString(bytes);
        await Task.CompletedTask; //Placeholder for actual async work
        return data;
    }
}
```

Go

Kit SDK pour Go V2

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement Kinesis avec Lambda à l'aide de Go.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package main
```

```
import (
 "context"
 "log"

 "github.com/aws/aws-lambda-go/events"
 "github.com/aws/aws-lambda-go/lambda"
)

func handler(ctx context.Context, kinesisEvent events.KinesisEvent) error {
 if len(kinesisEvent.Records) == 0 {
  log.Printf("empty Kinesis event received")
  return nil
 }

 for _, record := range kinesisEvent.Records {
  log.Printf("processed Kinesis event with EventId: %v", record.EventID)
  recordDataBytes := record.Kinesis.Data
  recordDataText := string(recordDataBytes)
  log.Printf("record data: %v", recordDataText)
  // TODO: Do interesting work based on the new data
 }
 log.Printf("successfully processed %v records", len(kinesisEvent.Records))
 return nil
}

func main() {
 lambda.Start(handler)
}
```

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement Kinesis avec Lambda à l'aide de Java.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package example;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.LambdaLogger;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.KinesisEvent;

public class Handler implements RequestHandler<KinesisEvent, Void> {
    @Override
    public Void handleRequest(final KinesisEvent event, final Context context) {
        LambdaLogger logger = context.getLogger();
        if (event.getRecords().isEmpty()) {
            logger.log("Empty Kinesis Event received");
            return null;
        }
        for (KinesisEvent.KinesisEventRecord record : event.getRecords()) {
            try {
                logger.log("Processed Event with EventId: "+record.getEventID());
                String data = new String(record.getKinesis().getData().array());
                logger.log("Data:"+ data);
                // TODO: Do interesting work based on the new data
            }
            catch (Exception ex) {
                logger.log("An error occurred:"+ex.getMessage());
                throw ex;
            }
        }
        logger.log("Successfully processed:"+event.getRecords().size()+"
 records");
        return null;
    }

}
```

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Utilisation d'un événement Kinesis avec Lambda à l'aide de. JavaScript

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
exports.handler = async (event, context) => {
  for (const record of event.Records) {
    try {
      console.log(`Processed Kinesis Event - EventID: ${record.eventID}`);
      const recordData = await getRecordDataAsync(record.kinesis);
      console.log(`Record Data: ${recordData}`);
      // TODO: Do interesting work based on the new data
    } catch (err) {
      console.error(`An error occurred ${err}`);
      throw err;
    }
  }
  console.log(`Successfully processed ${event.Records.length} records.`);
};

async function getRecordDataAsync(payload) {
  var data = Buffer.from(payload.data, "base64").toString("utf-8");
  await Promise.resolve(1); //Placeholder for actual async work
  return data;
}
```

Utilisation d'un événement Kinesis avec Lambda à l'aide de. TypeScript

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import {
  KinesisStreamEvent,
```

```
  Context,
  KinesisStreamHandler,
  KinesisStreamRecordPayload,
} from "aws-lambda";
import { Buffer } from "buffer";
import { Logger } from "@aws-lambda-powertools/logger";

const logger = new Logger({
  logLevel: "INFO",
  serviceName: "kinesis-stream-handler-sample",
});

export const functionHandler: KinesisStreamHandler = async (
  event: KinesisStreamEvent,
  context: Context
): Promise<void> => {
  for (const record of event.Records) {
    try {
      logger.info(`Processed Kinesis Event - EventID: ${record.eventID}`);
      const recordData = await getRecordDataAsync(record.kinesis);
      logger.info(`Record Data: ${recordData}`);
      // TODO: Do interesting work based on the new data
    } catch (err) {
      logger.error(`An error occurred ${err}`);
      throw err;
    }
    logger.info(`Successfully processed ${event.Records.length} records.`);
  }
};

async function getRecordDataAsync(
  payload: KinesisStreamRecordPayload
): Promise<string> {
  var data = Buffer.from(payload.data, "base64").toString("utf-8");
  await Promise.resolve(1); //Placeholder for actual async work
  return data;
}
```

PHP

Kit SDK pour PHP

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement Kinesis avec Lambda à l'aide de PHP.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
<?php

# using bref/bref and bref/logger for simplicity

use Bref\Context\Context;
use Bref\Event\Kinesis\KinesisEvent;
use Bref\Event\Kinesis\KinesisHandler;
use Bref\Logger\StderrLogger;

require __DIR__ . '/vendor/autoload.php';

class Handler extends KinesisHandler
{
    private StderrLogger $logger;
    public function __construct(StderrLogger $logger)
    {
        $this->logger = $logger;
    }

    /**
     * @throws JsonException
     * @throws \Bref\Event\InvalidLambdaEvent
     */
    public function handleKinesis(KinesisEvent $event, Context $context): void
    {
        $this->logger->info("Processing records");
        $records = $event->getRecords();
        foreach ($records as $record) {
            $data = $record->getData();
```

```
            $this->logger->info(json_encode($data));
            // TODO: Do interesting work based on the new data

            // Any exception thrown will be logged and the invocation will be
 marked as failed
        }
        $totalRecords = count($records);
        $this->logger->info("Successfully processed $totalRecords records");
    }
}

$logger = new StderrLogger();
return new Handler($logger);
```

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement Kinesis avec Lambda à l'aide de Python.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
import base64
def lambda_handler(event, context):

    for record in event['Records']:
        try:
            print(f"Processed Kinesis Event - EventID: {record['eventID']}")
            record_data = base64.b64decode(record['kinesis']
['data']).decode('utf-8')
            print(f"Record Data: {record_data}")
            # TODO: Do interesting work based on the new data
        except Exception as e:
            print(f"An error occurred {e}")
            raise e
```

```
    print(f"Successfully processed {len(event['Records'])} records.")
```

Ruby

Kit SDK pour Ruby

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement Kinesis avec Lambda à l'aide de Ruby.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
require 'aws-sdk'

def lambda_handler(event:, context:)
  event['Records'].each do |record|
    begin
      puts "Processed Kinesis Event - EventID: #{record['eventID']}"
      record_data = get_record_data_async(record['kinesis'])
      puts "Record Data: #{record_data}"
      # TODO: Do interesting work based on the new data
    rescue => err
      $stderr.puts "An error occurred #{err}"
      raise err
    end
  end
  puts "Successfully processed #{event['Records'].length} records."
end

def get_record_data_async(payload)
  data = Base64.decode64(payload['data']).force_encoding('UTF-8')
  # Placeholder for actual async work
  # You can use Ruby's asynchronous programming tools like async/await or fibers
 here.
  return data
end
```

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement Kinesis avec Lambda à l'aide de Rust.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
use aws_lambda_events::event::kinesis::KinesisEvent;
use lambda_runtime::{run, service_fn, Error, LambdaEvent};

async fn function_handler(event: LambdaEvent<KinesisEvent>) -> Result<(), Error>
 {
    if event.payload.records.is_empty() {
        tracing::info!("No records found. Exiting.");
        return Ok(());
    }

    event.payload.records.iter().for_each(|record| {
        tracing::info!("EventId:
 {}",record.event_id.as_deref().unwrap_or_default());

        let record_data = std::str::from_utf8(&record.kinesis.data);

        match record_data {
            Ok(data) => {
                // log the record data
                tracing::info!("Data: {}", data);
            }
            Err(e) => {
                tracing::error!("Error: {}", e);
            }
        }
    });

    tracing::info!(
        "Successfully processed {} records",
```

```
        event.payload.records.len()
    );

    Ok(())
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    tracing_subscriber::fmt()
        .with_max_level(tracing::Level::INFO)
        // disable printing the name of the module in every log line.
        .with_target(false)
        // disabling time is handy because CloudWatch will add the ingestion
 time.
        .without_time()
        .init();

    run(service_fn(function_handler)).await
}
```

Pour créer la fonction d'événement

1. Créez un répertoire pour le projet, puis passez à ce répertoire.

```
mkdir kinesis-tutorial
cd kinesis-tutorial
```

2. Copiez l'exemple de JavaScript code dans un nouveau fichier nomméindex.js.
3. Créez un package de déploiement.

```
zip function.zip index.js
```

4. Créez une fonction d'événement Lambda à l'aide de la `create-function` commande.

```
aws lambda create-function --function-name ProcessKinesisRecords \
--zip-file fileb://function.zip --handler index.handler --runtime nodejs24.x \
--role arn:aws:iam::111122223333:role/lambda-kinesis-role
```

Tester la fonction d'événement Lambda

Appelez manuellement votre fonction d'événement Lambda à l'aide de la commande `invoke` AWS Lambda CLI et d'un exemple d'événement Kinesis.

Pour tester la fonction d'événement Lambda

1. Copiez le code JSON suivant dans un fichier et enregistrez-le sous le nom `input.txt`.

```
{
    "Records": [
        {
            "kinesis": {
                "kinesisSchemaVersion": "1.0",
                "partitionKey": "1",
                "sequenceNumber":
 "49590338271490256608559692538361571095921575989136588898",
                "data": "SGVsbG8sIHRoaXMgaXMgYSB0ZXN0Lg==",
                "approximateArrivalTimestamp": 1545084650.987
            },
            "eventSource": "aws:kinesis",
            "eventVersion": "1.0",
            "eventID":
 "shardId-000000000006:49590338271490256608559692538361571095921575989136588898",
            "eventName": "aws:kinesis:record",
            "invokeIdentityArn": "arn:aws:iam::111122223333:role/lambda-kinesis-
role",
            "awsRegion": "us-east-2",
            "eventSourceARN": "arn:aws:kinesis:us-east-2:111122223333:stream/
lambda-stream"
        }
    ]
}
```

2. Utilisez la commande `invoke` pour envoyer l'événement à la fonction.

```
aws lambda invoke --function-name ProcessKinesisRecords \
--cli-binary-format raw-in-base64-out \
--payload file://input.txt outputfile.txt
```

L'cli-binary-formatoption est obligatoire si vous utilisez AWS CLI la version 2. Pour faire de ce paramètre le paramètre par défaut, exécutez `aws configure set cli-binary-format`

`raw-in-base64-out`. Pour plus d'informations, consultez les options de ligne de commande globales AWS CLI prises en charge dans le Guide de l'utilisateur AWS Command Line Interface version 2.

La réponse est enregistrée dans `out.txt`.

Créez un flux Kinesis

Pour créer un flux, utilisez la commande `create-stream` .

```
aws kinesis create-stream --stream-name lambda-stream --shard-count 1
```

Exécutez la commande `describe-stream` suivante pour obtenir l'ARN du flux.

```
aws kinesis describe-stream --stream-name lambda-stream
```

Vous devriez voir la sortie suivante :

```
{
    "StreamDescription": {
        "Shards": [
            {
                "ShardId": "shardId-000000000000",
                "HashKeyRange": {
                    "StartingHashKey": "0",
                    "EndingHashKey": "340282366920746074317682119384634633455"
                },
                "SequenceNumberRange": {
                    "StartingSequenceNumber":
 "49591073947768692513481539594623130411957558361251844610"
                }
            }
        ],
        "StreamARN": "arn:aws:kinesis:us-east-1:111122223333:stream/lambda-stream",
        "StreamName": "lambda-stream",
        "StreamStatus": "ACTIVE",
        "RetentionPeriodHours": 24,
        "EnhancedMonitoring": [
            {
                "ShardLevelMetrics": []
            }
```

```
        ],
        "EncryptionType": "NONE",
        "KeyId": null,
        "StreamCreationTimestamp": 1544828156.0
    }
}
```

Vous utiliserez l'ARN du flux à l'étape suivante pour associer le flux à votre fonction d'événement Lambda.

Ajouter une source d'événement dans AWS Lambda

Exécutez la commande suivante AWS CLI `add-event-source`.

```
aws lambda create-event-source-mapping --function-name ProcessKinesisRecords \
--event-source  arn:aws:kinesis:us-east-1:111122223333:stream/lambda-stream \
--batch-size 100 --starting-position LATEST
```

Notez l'ID de mappage pour une utilisation ultérieure. Pour obtenir une liste des mappages de source d'événement, exécutez la commande suivante `list-event-source-mappings`.

```
aws lambda list-event-source-mappings --function-name ProcessKinesisRecords \
--event-source arn:aws:kinesis:us-east-1:111122223333:stream/lambda-stream
```

Dans la réponse, vous pouvez vérifier que la valeur d'état indique `enabled`. Les mappages de source d'événement peuvent être désactivés pour suspendre temporairement l'interrogation, ce qui entraîne la perte d'enregistrements.

Tester la configuration

Pour tester le mappage de source d'événement, ajoutez des enregistrements d'événements à votre flux Kinesis. La `--data` valeur est une chaîne que la CLI code en base64 avant de l'envoyer à Kinesis. Vous pouvez exécuter la même commande plus d'une fois pour ajouter plusieurs enregistrements dans le flux.

```
aws kinesis put-record --stream-name lambda-stream --partition-key 1 \
--data "Hello, this is a test."
```

Lambda utilise le rôle d'exécution pour lire les enregistrements du flux. Ensuite, il invoque votre fonction d'événement Lambda, en transmettant des lots d'enregistrements. La fonction décode les

données de chaque enregistrement et les enregistre, en envoyant le résultat à CloudWatch Logs. Affichez les journaux dans la console CloudWatch .

Nettoyage de vos ressources

Vous pouvez maintenant supprimer les ressources que vous avez créées pour ce didacticiel, sauf si vous souhaitez les conserver. En supprimant AWS les ressources que vous n'utilisez plus, vous évitez des frais inutiles pour votre Compte AWS.

Pour supprimer le rôle d'exécution

1. Ouvrez la page Roles (Rôles) de la console IAM.
2. Sélectionnez le rôle d'exécution que vous avez créé.
3. Sélectionnez Supprimer.
4. Saisissez le nom du rôle dans le champ de saisie de texte et choisissez Delete (Supprimer).

Pour supprimer la fonction d'événement Lambda

1. Ouvrez la page Event Functions de la console Lambda.
2. Sélectionnez la fonction d'événement que vous avez créée.
3. Sélectionnez Actions, Supprimer.
4. Saisissez **`confirm`** dans la zone de saisie de texte et choisissez Delete (Supprimer).

Pour supprimer le flux Kinesis

1. Connectez-vous à la console Kinesis Console de gestion AWS et ouvrez-la à l'adresse. https://console.aws.amazon.com/kinesis
2. Sélectionnez le flux que vous avez créé.
3. Sélectionnez Actions, Supprimer.
4. Saisissez **`delete`** dans le champ de saisie de texte.
5. Sélectionnez Supprimer.

Utilisation de Lambda avec Kubernetes

Vous pouvez déployer et gérer les fonctions d'événement Lambda avec l'API Kubernetes à l'aide de AWS Controllers for Kubernetes (ACK) ou de Crossplane.

AWS Contrôleurs pour Kubernetes (ACK)

Vous pouvez utiliser ACK pour déployer et gérer des AWS ressources à partir de l'API Kubernetes. Grâce à ACK, AWS fournit des contrôleurs personnalisés open source pour AWS des services tels que Lambda, Amazon Elastic Container Registry (Amazon ECR), Amazon Simple Storage Service (Amazon S3) et Amazon AI. SageMaker Chaque AWS service pris en charge possède son propre contrôleur personnalisé. Dans votre cluster Kubernetes, installez un contrôleur pour chaque AWS service que vous souhaitez utiliser. Créez ensuite une définition de ressource personnalisée (CRD) pour définir les AWS ressources.

Nous vous recommandons d'utiliser Helm 3.8 ou version ultérieure pour installer les contrôleurs ACK. Chaque contrôleur ACK est doté de ses propres Charts de Helm, qui installent le contrôleur, les CRD et les règles RBAC de Kubernetes. Pour plus d'informations, consultez Installer un contrôleur ACK dans la documentation ACK.

Après avoir créé la ressource personnalisée ACK, vous pouvez l'utiliser comme n'importe quel autre objet Kubernetes intégré. Par exemple, vous pouvez déployer et gérer les fonctions d'événement Lambda avec vos chaînes d'outils Kubernetes préférées, y compris kubectl.

Voici quelques exemples de cas d'utilisation pour le provisionnement des fonctions d'événement Lambda via ACK :

- Votre organisation utilise le contrôle d'accès basé sur les rôles (RBAC) et des rôles IAM pour les comptes de service afin de créer les limites des autorisations. Avec ACK, vous pouvez réutiliser ce modèle de sécurité pour Lambda sans avoir à créer d'autres utilisateurs et stratégies.
- Votre organisation dispose d'un DevOps processus pour déployer des ressources dans un cluster Amazon Elastic Kubernetes Service (Amazon EKS) à l'aide de manifestes Kubernetes. Avec ACK, vous pouvez utiliser un manifeste pour provisionner les fonctions d'événement Lambda sans créer d'infrastructure distincte sous forme de modèles de code.

Pour plus d'informations sur l'utilisation d'ACK, consultez le didacticiel Lambda dans la documentation ACK.

Crossplane

Crossplane est un projet open source de la Cloud Native Computing Foundation (CNCF) qui utilise Kubernetes pour gérer les ressources de l'infrastructure cloud. Avec Crossplane, les développeurs peuvent demander une infrastructure sans avoir à en comprendre la complexité. Les équipes chargées de la plateforme gardent le contrôle de la manière dont l'infrastructure est provisionnée et gérée.

À l'aide de Crossplane, vous pouvez déployer et gérer les fonctions d'événement Lambda avec vos chaînes d'outils Kubernetes préférées, telles que kubectl, et CI/CD avec tout pipeline capable de déployer des manifestes sur Kubernetes. Voici quelques exemples de cas d'utilisation pour le provisionnement de fonctions d'événement Lambda via Crossplane :

- Votre organisation souhaite renforcer la conformité en s'assurant que les fonctions d'événement Lambda disposent des balises appropriées. Les équipes chargées de la plateforme peuvent utiliser Compositions Crossplane pour définir cette stratégie par le biais d'abstractions d'API. Les développeurs peuvent ensuite utiliser ces abstractions pour déployer des fonctions d'événement Lambda avec des balises.
- Votre projet utilise GitOps Kubernetes. Dans ce modèle, Kubernetes réconcilie en permanence le référentiel Git (état souhaité) avec les ressources qui s'exécutent à l'intérieur du cluster (état actuel). En cas de différences, le GitOps processus apporte automatiquement des modifications au cluster. Vous pouvez utiliser GitOps Kubernetes pour déployer et gérer les fonctions d'événement Lambda via Crossplane, en utilisant des outils et des concepts Kubernetes familiers tels que les CRD et les contrôleurs.

Pour en savoir plus sur l'utilisation de Crossplane avec Lambda, consultez les rubriques suivantes :

- AWS Blueprints for Crossplane : ce référentiel contient des exemples d'utilisation de Crossplane pour déployer des AWS ressources, notamment des fonctions d'événement Lambda.

  > **Note**
  >
  > AWS Les plans pour Crossplane sont en cours de développement et ne devraient pas être utilisés en production.

- Déploiement de Lambda avec Amazon EKS et Crossplane : cette vidéo présente un exemple avancé de déploiement d'une architecture AWS sans serveur avec Crossplane, en explorant la conception du point de vue du développeur et du point de vue de la plateforme.

Utilisation de Lambda avec Amazon MQ

> **Note**
>
> Si vous souhaitez envoyer des données à une cible autre qu'une fonction d'événement Lambda ou enrichir les données avant de les envoyer, consultez Amazon EventBridge Pipes.

Amazon MQ est un service d'agent de messages géré pour Apache ActiveMQ et RabbitMQ. Un agent de messages permet à des applications et composants logiciels de communiquer à l'aide de divers langages de programmation, systèmes d'exploitation et autres protocoles de messagerie formels par le biais de rubriques ou d'événements en file d'attente.

Amazon MQ peut également gérer des instances Amazon Elastic Compute Cloud (Amazon EC2) en votre nom en installant des agents ActiveMQ ou RabbitMQ, et en fournissant différentes topologies réseau et infrastructures.

Vous pouvez utiliser une fonction d'événement Lambda pour traiter les enregistrements de votre courtier de messages Amazon MQ. Lambda invoque votre fonction via un mappage de source d'événement, une ressource Lambda qui lit les messages de votre agent et invoque la fonction de manière synchrone. Pour les options de configuration, voirthe section called "Paramètres". Pour les erreurs courantes, voirthe section called "Dépannage".

> **Warning**
>
> Les mappages des sources d'événements Lambda traitent chaque événement au moins une fois, et le traitement des enregistrements peut être dupliqué. Pour éviter les problèmes potentiels liés à des événements dupliqués, nous vous recommandons vivement de rendre votre code de fonction idempotent. Pour en savoir plus, consultez Comment rendre ma fonction Lambda idempotente dans le Knowledge Center. AWS

Le mappage de source d'événement Amazon MQ est sujet aux restrictions de configuration suivantes :

- Concurrence — Les fonctions d'événement Lambda qui utilisent un mappage de source d'événements Amazon MQ ont un paramètre de simultanéité maximale par défaut. Pour ActiveMQ, le service Lambda limite le nombre d'environnements d'exécution simultanés à cinq par mappage

des sources d'événements Amazon MQ. Pour RabbitMQ, le nombre d'environnements d'exécution simultanés est limité à 1 par mappage des sources d'événements Amazon MQ.

Même si vous modifiez les paramètres de simultanéité réservés ou fournis de votre fonction, le service Lambda ne mettra pas plus d'environnements d'exécution à disposition. Pour demander une augmentation de la simultanéité maximale par défaut pour un seul mappage de source d'événement Amazon MQ, Support contactez l'UUID du mappage de source d'événement, ainsi que la région. Étant donné que les augmentations sont appliquées au niveau de chaque mappage des sources d'événements, et non au niveau du compte ou de la région, vous devez demander manuellement une augmentation de mise à l'échelle pour chaque mappage des sources d'événements.

- Traitement entre comptes – Lambda ne prend pas en charge le traitement entre comptes. Vous ne pouvez pas utiliser Lambda pour traiter des enregistrements d'un agent de messages Amazon MQ se trouvant dans un autre Compte AWS.
- Authentification — Pour ActiveMQ, seul ActiveMQ est pris en charge. SimpleAuthenticationPlugin Pour RabbitMQ, seule l'authentification PLAIN est prise en charge. Les utilisateurs doivent utiliser AWS Secrets Manager pour gérer leurs informations d'identification. Pour plus d'informations sur l'authentification ActiveMQ, consultez Intégration d'agents ActiveMQ avec LDAP dans le Guide du développeur Amazon MQ.
- Quota de connexion – Les agents ont un nombre maximum de connexions autorisées par protocole de niveau filaire. Ce quota est basé sur le type d'instance de l'agent. Pour plus d'informations, consultez la section Agents de Quotas dans Amazon dans le Manuel du développeur Amazon MQ.
- Connectivité – Vous pouvez créer des agents dans un cloud privé virtuel (VPC) public ou privé. Pour les VPC privés, votre fonction d'événement Lambda doit accéder au VPC pour recevoir des messages. Pour plus d'informations, consultez the section called "Configurer la sécurité réseau", plus loin dans cette section.
- Destinations d'événements – Seules les destinations en file d'attente sont prises en charge. Toutefois, vous pouvez utiliser une rubrique virtuelle qui se comporte comme une rubrique en interne tout en interagissant avec Lambda en tant que file d'attente. Pour plus d'informations, consultez Virtual Destinations (Destinations virtuelles) sur le site web Apache ActiveMQ, et Virtual Hosts (Hôtes virtuels) sur le site web RabbitMQ.
- Topologie réseau – Pour ActiveMQ, un mappage de source d'événement prend en charge une seule instance ou un seul agent en veille. Pour RabbitMQ, un seul déploiement de broker ou de cluster à instance unique est pris en charge par mappage de source d'événement. Single-instance les courtiers ont besoin d'un point de terminaison de basculement. Pour plus d'informations sur ces

modes de déploiement d'agent, consultez Architecture d'agent ActiveMQ et Architecture d'agent RabbitMQ dans le Guide du développeur Amazon MQ.

- Protocoles – Les protocoles pris en charge dépendent du type d'intégration d'Amazon MQ.
  - Pour les intégrations ActiveMQ, Lambda consomme les messages à l'aide OpenWire/Java du protocole Message Service (JMS). Aucun autre protocole n'est pris en charge pour la consommation de messages. Dans le protocole JMS, seuls `TextMessage` et `BytesMessage` sont pris en charge. Lambda prend également en charge les propriétés personnalisées JMS. Pour plus d'informations sur le OpenWire protocole, consultez OpenWirele site Web d'Apache ActiveMQ.
  - Pour les intégrations RabbitMQ, Lambda consomme des messages à l'aide du protocole AMQP 0-9-1. Aucun autre protocole n'est pris en charge pour la consommation de messages. Pour plus d'informations sur l'implémentation par RabbitMQ du protocole AMQP 0-9-1, consultez Guide de référence complet AMQP 0-9-1 sur le site web de RabbitMQ.

Lambda prend automatiquement en charge les dernières versions d'ActiveMQ et de RabbitMQ qu'Amazon MQ prend en charge. Pour connaître les dernières versions prises en charge, consultez Notes de mise à jour Amazon MQ dans le Guide du développeur Amazon MQ.

> **Note**
>
> Par défaut, Amazon MQ comporte une fenêtre de maintenance hebdomadaire pour les agents. Pendant cette période, les agents ne sont pas disponibles. Pendant ce temps, Lambda ne peut pas traiter les messages des agents sans veille.

Rubriques

- Comprendre le groupe de consommateurs Lambda pour Amazon MQ
- Configuration de source d'événements Amazon MQ pour Lambda
- Paramètres de mappage des sources d'événements
- Filtrer les événement à partir d'une source d'événements Amazon MQ
- Résoudre les erreurs de mappage des sources d'événement Amazon MQ

Comprendre le groupe de consommateurs Lambda pour Amazon MQ

Pour interagir avec Amazon MQ, Lambda crée un groupe de consommateurs qui peut être lu à partir de vos agents Amazon MQ. Le groupe de consommateurs est créé avec le même ID qu'un mappage de source d'événements UUID.

Pour les sources d'événements Amazon MQ, Lambda réunit les enregistrements par lots et les envoie à votre fonction dans une seule charge utile. Pour contrôler le comportement, vous pouvez configurer la fenêtre de traitement par lots et la taille du lot. Lambda extrait les messages jusqu'à ce qu'il traite la taille maximale de la charge utile de 6 Mo, que la fenêtre de traitement par lots expire ou que le nombre d'enregistrements atteigne la taille totale du lot. Pour plus d'informations, consultez Comportement de traitement par lots.

Le groupe de consommateurs récupère les messages sous forme de BLOB d'octets, puis les code en base64 dans une charge unique JSON puis invoque votre fonction. Si votre fonction renvoie une erreur pour l'un des messages d'un lot, Lambda réessaie le lot de messages complet jusqu'à ce que le traitement réussisse ou que les messages expirent.

> **Note**
>
> Alors que les fonctions d'événement Lambda ont généralement un délai d'expiration maximal de 15 minutes, les mappages de sources d'événements pour Amazon MSK, Apache Kafka autogéré, Amazon DocumentDB et Amazon MQ pour ActiveMQ et RabbitMQ ne prennent en charge que les fonctions dont le délai d'expiration maximal est de 14 minutes. Cette contrainte garantit que le mappage des sources d'événements peut gérer correctement les erreurs de fonction et effectuer de nouvelles tentatives.

Vous pouvez surveiller l'utilisation simultanée d'une fonction donnée à l'aide de la `ConcurrentExecutions` métrique d'Amazon CloudWatch. Pour de plus amples informations sur la simultanéité, consultez the section called "Configuration de la simultanéité réservée".

ExampleÉvénements d'enregistrement Amazon MQ

ActiveMQ

```
{
   "eventSource": "aws:mq",
   "eventSourceArn": "arn:aws:mq:us-
east-2:111122223333:broker:test:b-9bcfa592-423a-4942-879d-eb284b418fc8",
```

```
   "messages": [
      {
        "messageID": "ID:b-9bcfa592-423a-4942-879d-eb284b418fc8-1.mq.us-
east-2.amazonaws.com-37557-1234520418293-4:1:1:1:1",
        "messageType": "jms/text-message",
        "deliveryMode": 1,
        "replyTo": null,
        "type": null,
        "expiration": "60000",
        "priority": 1,
        "correlationId": "myJMSCoID",
        "redelivered": false,
        "destination": {
          "physicalName": "testQueue"
        },
        "data":"QUJDOkFBQUE=",
        "timestamp": 1598827811958,
        "brokerInTime": 1598827811958,
        "brokerOutTime": 1598827811959,
        "properties": {
          "index": "1",
          "doAlarm": "false",
          "myCustomProperty": "value"
        }
      },
      {
        "messageID": "ID:b-9bcfa592-423a-4942-879d-eb284b418fc8-1.mq.us-
east-2.amazonaws.com-37557-1234520418293-4:1:1:1:1",
        "messageType": "jms/bytes-message",
        "deliveryMode": 1,
        "replyTo": null,
        "type": null,
        "expiration": "60000",
        "priority": 2,
        "correlationId": "myJMSCoID1",
        "redelivered": false,
        "destination": {
          "physicalName": "testQueue"
        },
        "data":"LQaGQ82S48k=",
        "timestamp": 1598827811958,
        "brokerInTime": 1598827811958,
        "brokerOutTime": 1598827811959,
        "properties": {
```

```
          "index": "1",
          "doAlarm": "false",
          "myCustomProperty": "value"
        }
      }
   ]
}
```

RabbitMQ

```
{
  "eventSource": "aws:rmq",
  "eventSourceArn": "arn:aws:mq:us-
east-2:111122223333:broker:pizzaBroker:b-9bcfa592-423a-4942-879d-eb284b418fc8",
  "rmqMessagesByQueue": {
    "pizzaQueue::/": [
      {
        "basicProperties": {
          "contentType": "text/plain",
          "contentEncoding": null,
          "headers": {
            "header1": {
              "bytes": [
                118,
                97,
                108,
                117,
                101,
                49
              ]
            },
            "header2": {
              "bytes": [
                118,
                97,
                108,
                117,
                101,
                50
              ]
            },
            "numberInHeader": 10
```

```
          },
          "deliveryMode": 1,
          "priority": 34,
          "correlationId": null,
          "replyTo": null,
          "expiration": "60000",
          "messageId": null,
          "timestamp": "Jan 1, 1970, 12:33:41 AM",
          "type": null,
          "userId": "AIDACKCEVSQ6C2EXAMPLE",
          "appId": null,
          "clusterId": null,
          "bodySize": 80
        },
        "redelivered": false,
        "data": "eyJ0aW1lb3V0IjowLCJkYXRhIjoiQ1pybWYwR3c4T3Y0YnFMUXhENEUifQ=="
      }
    ]
  }
}
```

> **Note**
>
> Dans l'exemple RabbitMQ, `pizzaQueue` est le nom de la file d'attente RabbitMQ, et `/` est le nom de l'hôte virtuel. Lors de la réception de messages, la source d'événement répertorie les messages sous `pizzaQueue::/`.

Configuration de source d'événements Amazon MQ pour Lambda

Rubriques

- Configurer la sécurité réseau
- Créer le mappage des sources d'événements

Configurer la sécurité réseau

Pour donner à Lambda un accès complet à Amazon MQ via votre mappage des sources d'événements, soit votre agent doit utiliser un point de terminaison public (adresse IP publique), soit vous devez fournir un accès au VPC Amazon dans lequel vous avez créé l'agent.

Lorsque vous utilisez Amazon MQ avec Lambda, créez des points de terminaison AWS PrivateLink VPC qui permettent à votre fonction d'événement d'accéder aux ressources de votre Amazon VPC.

> **Note**
>
> AWS PrivateLink Les points de terminaison VPC sont requis pour les fonctions avec des mappages de sources d'événements qui utilisent le mode par défaut (à la demande) pour les sondeurs d'événements. Si le mappage de votre source d'événements utilise le mode provisionné, vous n'avez pas besoin de configurer les points de terminaison AWS PrivateLink VPC.

Créez un point de terminaison pour accéder aux ressources suivantes :

- Lambda — Créez un point de terminaison pour le principal de service Lambda.
- AWS STS — Créez un point de terminaison pour le AWS STS afin qu'un directeur de service assume un rôle en votre nom.
- Secrets Manager : si votre agent utilise Secrets Manager pour stocker les informations d'identification, créez un point de terminaison pour Secrets Manager.

Vous pouvez également configurer une passerelle NAT sur chaque sous-réseau public d'Amazon VPC. Pour plus d'informations, consultez the section called “Accès Internet pour les fonctions VPC”.

Lorsque vous créez un mappage des sources d'événements pour Amazon MQ, Lambda vérifie si des interfaces réseau Elastic (ENI) sont déjà présentes pour les sous-réseaux et les groupes de sécurité configurés pour votre VPC Amazon. Si Lambda trouve des ENI existantes, il tente de les réutiliser. Sinon, Lambda crée de nouvelles ENI pour se connecter à la source d'événement et invoquer votre fonction.

> **Note**
>
> Les fonctions d'événement Lambda s'exécutent toujours dans des VPC appartenant au service Lambda. La configuration VPC de votre fonction n'affecte pas le mappage des sources d'événements. Seule la configuration réseau des sources d'événements détermine la manière dont Lambda se connecte à votre source d'événements.

Configurez les groupes de sécurité pour le VPC Amazon contenant votre agent. Par défaut, Amazon MQ utilise les ports suivants : 61617 (Amazon MQ pour ActiveMQ) 5671 et (Amazon MQ pour RabbitMQ).

- Règles entrantes – Autorisent tout le trafic sur le port de l'agent par défaut pour le groupe de sécurité associé à votre source d'événement. Vous pouvez également utiliser une règle de groupe de sécurité avec référence circulaire pour autoriser l'accès à partir d'instances appartenant au même groupe de sécurité.
- Règles de sortie : autorisez tout le trafic sur le port 443 pour les destinations externes si votre fonction doit communiquer avec les AWS services. Vous pouvez également utiliser une règle de groupe de sécurité à référencement automatique pour limiter l'accès au courtier si vous n'avez pas besoin de communiquer avec d'autres AWS services.
- Règles entrantes relatives au point de terminaison Amazon VPC – Si vous utilisez un point de terminaison Amazon VPC, le groupe de sécurité associé à votre point de terminaison Amazon VPC doit autoriser le trafic entrant sur le port 443 en provenance du groupe de sécurité de l'agent.

Si votre agent utilise l'authentification, vous pouvez également restreindre la politique de point de terminaison pour le point de terminaison Secrets Manager. Pour appeler l'API Secrets Manager, Lambda utilise votre rôle de fonction, et non le principal de service Lambda.

Example Politique de point de terminaison de VPC — Point de terminaison Secrets Manager

```
{
      "Statement": [
          {
              "Action": "secretsmanager:GetSecretValue",
              "Effect": "Allow",
              "Principal": {
                  "AWS": [
                      "arn:aws::iam::123456789012:role/my-role"
                  ]
              },
              "Resource": "arn:aws::secretsmanager:us-west-2:123456789012:secret:my-
secret"
          }
      ]
  }
```

Lorsque vous utilisez des points de terminaison Amazon VPC, AWS achemine vos appels d'API pour appeler votre fonction à l'aide de l'Elastic Network Interface (ENI) du point de terminaison. Le principal de service Lambda doit appeler `lambda:InvokeFunction` pour tous les rôles et fonctions utilisant ces ENI.

Par défaut, les points de terminaison Amazon VPC disposent de politiques IAM ouvertes qui permettent un accès étendu aux ressources. La meilleure pratique consiste à restreindre ces politiques pour effectuer les actions nécessaires à l'aide de ce point de terminaison. Pour garantir que le mappage de votre source d'événements est en mesure d'appeler votre fonction d'événement Lambda, la politique de point de terminaison VPC doit autoriser le principal du service Lambda à appeler et. `sts:AssumeRole` `lambda:InvokeFunction` Le fait de restreindre vos politiques de point de terminaison de VPC pour autoriser uniquement les appels d'API provenant de votre organisation empêche le mappage des sources d'événements de fonctionner correctement. C'est pourquoi `"Resource": "*"` est requis dans ces politiques.

Les exemples de politiques de point de terminaison de VPC suivants montrent comment accorder l'accès requis au principal de service Lambda pour les points de terminaison AWS STS et Lambda.

Example Politique relative aux points de terminaison VPC — AWS STS point de terminaison

```
{
      "Statement": [
          {
              "Action": "sts:AssumeRole",
              "Effect": "Allow",
              "Principal": {
                  "Service": [
                      "lambda.amazonaws.com"
                  ]
              },
              "Resource": "*"
          }
      ]
    }
```

Example Politique de point de terminaison de VPC — Point de terminaison Lambda

```
{
      "Statement": [
          {
              "Action": "lambda:InvokeFunction",
```

```
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "lambda.amazonaws.com"
                ]
            },
            "Resource": "*"
        }
    ]
}
```

Créer le mappage des sources d’événements

Créez un mappage de source d'événements pour indiquer à Lambda d'envoyer des enregistrements depuis un courtier Amazon MQ vers une fonction d'événement Lambda. Vous pouvez créer plusieurs mappages de source d’événement pour traiter les mêmes données avec plusieurs fonctions, ou pour traiter des éléments à partir de plusieurs sources avec une seule fonction.

Pour configurer votre fonction afin qu’elle lise à partir d’Amazon MQ, ajoutez les autorisations requises et créez un déclencheur MQ dans la console Lambda.

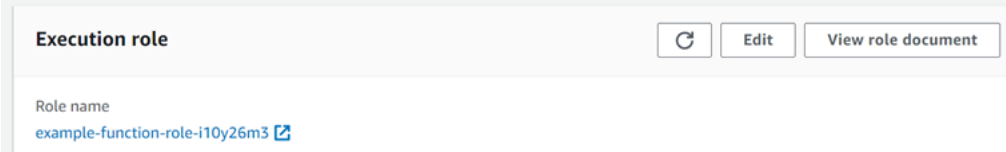
Pour lire les enregistrements d'un courtier Amazon MQ, votre fonction d'événement Lambda a besoin des autorisations suivantes. Vous autorisez Lambda à interagir avec votre agent Amazon MQ et ses ressources sous-jacentes en ajoutant des déclarations d’autorisation à votre rôle d’exécution de fonction :

- mq : DescribeBroker
- responsable des secrets : GetSecretValue
- EC2 : CreateNetworkInterface
- EC2 : DeleteNetworkInterface
- EC2 : DescribeNetworkInterfaces
- EC2 : DescribeSecurityGroups
- EC2 : DescribeSubnets
- EC2 : DescribeVpcs
- journaux : CreateLogGroup
- journaux : CreateLogStream
- journaux : PutLogEvents

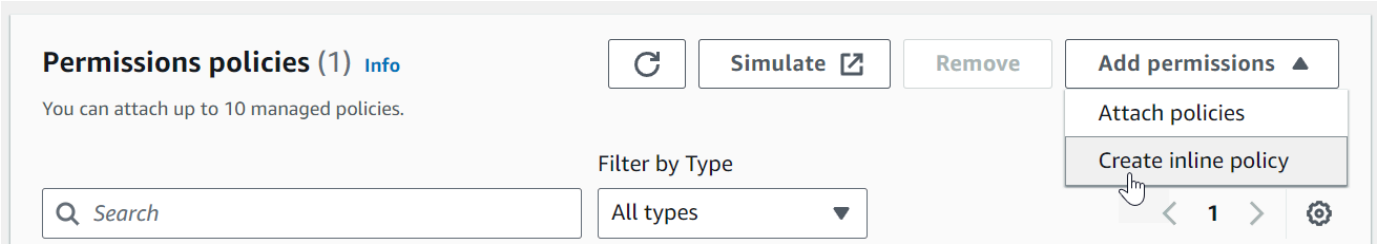
> **Note**
>
> Lorsque vous utilisez une clé gérée par le client chiffrée, ajoutez également l'autorisation `kms:Decrypt`.

Pour ajouter des autorisations et créer un déclencheur

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez le nom d'une fonction.
3. Choisissez l'onglet Configuration, puis Permissions (Autorisations).
4. Sous Nom du rôle, cliquez sur le lien vers votre rôle d'exécution. Ce lien ouvre le rôle dans la console IAM.



5. Sélectionnez Ajouter des autorisations, puis Ajouter la politique.



6. Dans l'Éditeur de politique, sélectionnez JSON. Saisissez la politique suivante. Votre fonction a besoin de ces autorisations pour lire à partir d'un agent Amazon MQ.

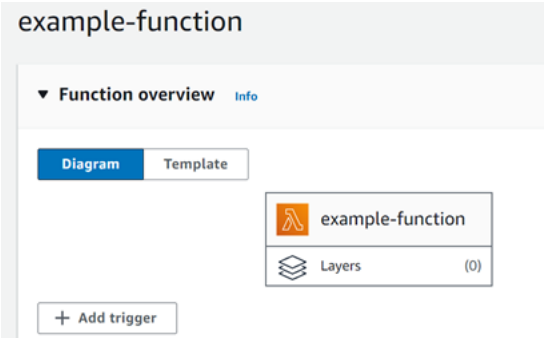
   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
          "mq:DescribeBroker",
          "secretsmanager:GetSecretValue",
          "ec2:CreateNetworkInterface",
```

```
            "ec2:DeleteNetworkInterface",
            "ec2:DescribeNetworkInterfaces",
            "ec2:DescribeSecurityGroups",
            "ec2:DescribeSubnets",
            "ec2:DescribeVpcs",
            "logs:CreateLogGroup",
            "logs:CreateLogStream",
            "logs:PutLogEvents"
        ],
        "Resource": "*"
    }
  ]
}
```

> **Note**
>
> Lorsque vous utilisez une clé gérée par le client chiffrée, vous devez également ajouter l'autorisation `kms:Decrypt`.

7. Choisissez Suivant. Saisissez un nom de politique, puis choisissez Créer une politique.
8. Revenez à votre fonction dans la console Lambda. Sous Function overview (Vue d'ensemble de la fonction), choisissez Add trigger (Ajouter un déclencheur).



9. Choisissez le type de déclencheur MQ.
10. Configurez les options requises, puis choisissez Add (Ajouter).

Lambda prend en charge les options suivantes pour les sources d'événement Amazon MQ.

- MQ broker (Agent MQ) – Sélectionnez un agent Amazon MQ.
- Batch size (Taille de lot) – Définissez le nombre maximum de messages à extraire dans un lot.

- Queue name (Nom de file d'attente) – Entrez la file d'attente Amazon MQ à consommer.
- Source access configuration (Configuration de l'accès source) – Entrez les informations d'hôte virtuel et le secret Secrets Manager qui stocke vos informations d'identification d'agent.
- Enable trigger (Activer le déclencheur) – Désactivez le déclencheur pour arrêter le traitement des enregistrements.

Pour activer ou désactiver le déclencheur (ou le supprimer), choisissez le déclencheur MQ dans le concepteur. Pour reconfigurer le déclencheur, utilisez les opérations d'API de mappage de source d'événement.

Paramètres de mappage des sources d'événements

Tous les types de sources d'événement Lambda partagent les mêmes opérations d'API CreateEventSourceMapping et UpdateEventSourceMapping. Cependant, seuls certains paramètres s'appliquent à Amazon MQ et à RabbitMQ.

Paramètre	Obligatoire	Par défaut	Remarques
BatchSize	N	100	Maximum : 10 000.
Activé	N	VRAI	none
FunctionName	Y	N/A	none
FilterCriteria	N	N/A	Contrôlez les événements que Lambda envoie à votre fonction d'événement
MaximumBatchingWindowInSeconds	N	500 ms	Comportement de traitement par lots
Files d'attente	N	N/A	Le nom de la file d'attente de destination de l'agent Amazon MQ à consommer.

Paramètre	Obligatoire	Par défaut	Remarques
SourceAccessConfigurations	N	N/A	Pour ActiveMQ, informations d'identification BASIC_AUTH. Pour RabbitMQ, il peut contenir à la fois des informations d'identification BASIC_AUTH et des informations VIRTUAL_HOST.

Filtrer les événement à partir d'une source d'événements Amazon MQ

Vous pouvez utiliser le filtrage des événements pour contrôler les enregistrements d'un flux ou d'une file d'attente que Lambda envoie à votre fonction d'événement. Pour obtenir des informations générales sur le fonctionnement du filtrage des événements, consultez the section called "Filtrage des événements".

Cette section porte sur le filtrage des événements pour les sources Amazon MQ.

> **Note**
>
> Les mappages des sources d'événements Amazon MQ prennent uniquement en charge le filtrage sur la clé `data`.

Rubriques

- Principes de base du filtrage des événements Amazon MQ

Principes de base du filtrage des événements Amazon MQ

Supposons que votre file d'attente de messages Amazon MQ contienne des messages au format JSON valide ou sous forme de chaînes simples. Un exemple d'enregistrement ressemblerait à ce qui suit, avec les données converties en chaîne encodée en Base64 dans le champ `data`.

ActiveMQ

```
{
    "messageID": "ID:b-9bcfa592-423a-4942-879d-eb284b418fc8-1.mq.us-
east-2.amazonaws.com-37557-1234520418293-4:1:1:1:1",
    "messageType": "jms/text-message",
    "deliveryMode": 1,
    "replyTo": null,
    "type": null,
    "expiration": "60000",
    "priority": 1,
    "correlationId": "myJMSCoID",
    "redelivered": false,
    "destination": {
      "physicalName": "testQueue"
    },
    "data":"QUJDOkFBQUE=",
    "timestamp": 1598827811958,
    "brokerInTime": 1598827811958,
    "brokerOutTime": 1598827811959,
    "properties": {
      "index": "1",
      "doAlarm": "false",
      "myCustomProperty": "value"
    }
}
```

RabbitMQ

```
{
    "basicProperties": {
        "contentType": "text/plain",
        "contentEncoding": null,
        "headers": {
            "header1": {
                "bytes": [
                  118,
                  97,
                  108,
                  117,
                  101,
                  49
                ]
```

```
            },
            "header2": {
                "bytes": [
                  118,
                  97,
                  108,
                  117,
                  101,
                  50
                ]
            },
            "numberInHeader": 10
        },
        "deliveryMode": 1,
        "priority": 34,
        "correlationId": null,
        "replyTo": null,
        "expiration": "60000",
        "messageId": null,
        "timestamp": "Jan 1, 1970, 12:33:41 AM",
        "type": null,
        "userId": "AIDACKCEVSQ6C2EXAMPLE",
        "appId": null,
        "clusterId": null,
        "bodySize": 80
        },
    "redelivered": false,
    "data": "eyJ0aW1lb3V0IjowLCJkYXRhIjoiQ1pybWYwR3c4T3Y0YnFMUXhENEUifQ=="
}
```

Pour les agents Active MQ et Rabbit MQ, vous pouvez utiliser le filtrage d'événements pour filtrer les enregistrements à l'aide de la clé `data`. Supposons que votre file d'attente Amazon MQ contienne des messages au format JSON suivant.

```
{
    "timeout": 0,
    "IPAddress": "203.0.113.254"
}
```

Pour filtrer uniquement les enregistrements dont le champ `timeout` est supérieur à 0, l'objet `FilterCriteria` serait le suivant.

```
{
    "Filters": [
        {
            "Pattern": "{ \"data\" : { \"timeout\" : [ { \"numeric\": [ \">\",
 0] } } ] } }"
        }
    ]
}
```

Pour plus de clarté, voici la valeur du `Pattern` de filtre étendu en JSON simple :

```
{
    "data": {
        "timeout": [ { "numeric": [ ">", 0 ] } ]
        }
}
```

Vous pouvez ajouter votre filtre à l'aide de la console AWS CLI ou d'un AWS SAM modèle.

Console

pour ajouter ce filtre à l'aide de la console, suivez les instructions de Attacher des critères de filtre à un mappage de sources d'événements (console) et saisissez la chaîne suivante comme critère de filtre.

```
{ "data" : { "timeout" : [ { "numeric": [ ">", 0 ] } ] } }
```

AWS CLI

Pour créer un nouveau mappage de source d'événements avec ces critères de filtre à l'aide de AWS Command Line Interface (AWS CLI), exécutez la commande suivante.

```
aws lambda create-event-source-mapping \
    --function-name my-function \
    --event-source-arn arn:aws:mq:us-east-2:123456789012:broker:my-
broker:b-8ac7cc01-5898-482d-be2f-a6b596050ea8 \
    --filter-criteria '{"Filters": [{"Pattern": "{ \"data\" : { \"timeout\" :
 [ { \"numeric\": [ \">\", 0 ] } ] } }"}]}'
```

Pour ajouter ces critères de filtre à un mappage des sources d'événements existant, exécutez la commande suivante.

```
aws lambda update-event-source-mapping \
    --uuid "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE" \
    --filter-criteria '{"Filters": [{"Pattern": "{ \"data\" : { \"timeout\" :
 [ { \"numeric\": [ \">\", 0 ] } ] } }"}]}'
```

Pour ajouter ces critères de filtre à un mappage des sources d'événements existant, exécutez la commande suivante.

```
aws lambda update-event-source-mapping \
    --uuid "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE" \
    --filter-criteria '{"Filters": [{"Pattern": "{ \"data\" : { \"timeout\" :
 [ { \"numeric\": [ \">\", 0 ] } ] } }"}]}'
```

AWS SAM

Pour ajouter ce filtre AWS SAM, ajoutez l'extrait suivant au modèle YAML de votre source d'événement.

```
FilterCriteria:
  Filters:
    - Pattern: '{ "data" : { "timeout" : [ { "numeric": [ ">", 0 ] } ] } }'
```

Avec Amazon MQ, vous pouvez également filtrer les enregistrements dont le message est une chaîne simple. Supposons que vous vouliez traiter uniquement les enregistrements dont le message commence par « Result: ». L'objet `FilterCriteria` se présente comme suit.

```
{
    "Filters": [
        {
            "Pattern": "{ \"data\" : [ { \"prefix\": \"Result: \" } ] }"
        }
    ]
}
```

Pour plus de clarté, voici la valeur du `Pattern` de filtre étendu en JSON simple :

```
{
    "data": [
        {
        "prefix": "Result: "
```

```
        }
    ]
}
```

Vous pouvez ajouter votre filtre à l'aide de la console AWS CLI ou d'un AWS SAM modèle.

Console

Pour ajouter ce filtre à l'aide de la console, suivez les instructions de Attacher des critères de filtre à un mappage de sources d'événements (console) et saisissez la chaîne suivante comme critère de filtre.

```
{ "data" : [ { "prefix": "Result: " } ] }
```

AWS CLI

Pour créer un nouveau mappage de source d'événements avec ces critères de filtre à l'aide de AWS Command Line Interface (AWS CLI), exécutez la commande suivante.

```
aws lambda create-event-source-mapping \
    --function-name my-function \
    --event-source-arn arn:aws:mq:us-east-2:123456789012:broker:my-
broker:b-8ac7cc01-5898-482d-be2f-a6b596050ea8 \
    --filter-criteria '{"Filters": [{"Pattern": "{ \"data\" : [ { \"prefix\":
 \"Result: \" } ] }"}]}'
```

Pour ajouter ces critères de filtre à un mappage des sources d'événements existant, exécutez la commande suivante.

```
aws lambda update-event-source-mapping \
    --uuid "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE" \
    --filter-criteria '{"Filters": [{"Pattern": "{ \"data\" : [ { \"prefix\":
 \"Result: \" } ] }"}]}'
```

AWS SAM

Pour ajouter ce filtre AWS SAM, ajoutez l'extrait suivant au modèle YAML de votre source d'événement.

```
FilterCriteria:
  Filters:
```

```
    - Pattern: '{ "data" : [ { "prefix": "Result " } ] }'
```

Les messages Amazon MQ doivent être des chaînes UTF-8 codées, soit des chaînes simples, soit au format JSON. Cela est dû au fait que Lambda décode les tableaux d'octets Amazon MQ avant d'appliquer les critères de filtrage. UTF-8 Si vos messages utilisent un autre encodage, tel que UTF-16 l'ASCII, ou si le format du message ne correspond pas au format, Lambda traite uniquement les `FilterCriteria` filtres de métadonnées. Le tableau suivant résume le comportement spécifique :

Format du du message entrant	Modèle de filtre de format pour les propriétés des messages	Action obtenue.
Chaîne de texte brut	Chaîne de texte brut	Lambda filtre en fonction de vos critères de filtre.
Chaîne de texte brut	Pas de modèle de filtre pour les propriétés des données	Lambda filtre (uniquement selon les autres propriétés de métadonnées) en fonction de vos critères de filtre.
Chaîne de texte brut	JSON valide	Lambda filtre (uniquement selon les autres propriétés de métadonnées) en fonction de vos critères de filtre.
JSON valide	Chaîne de texte brut	Lambda filtre (uniquement selon les autres propriétés de métadonnées) en fonction de vos critères de filtre.
JSON valide	Pas de modèle de filtre pour les propriétés des données	Lambda filtre (uniquement selon les autres propriétés de métadonnées) en fonction de vos critères de filtre.
JSON valide	JSON valide	Lambda filtre en fonction de vos critères de filtre.

Format du du message entrant	Modèle de filtre de format pour les propriétés des messages	Action obtenue.
Non-UTF-8 chaîne codée	JSON, chaîne de texte brut ou aucun modèle	Lambda filtre (uniquement selon les autres propriétés de métadonnées) en fonction de vos critères de filtre.

Résoudre les erreurs de mappage des sources d'événement Amazon MQ

Lorsqu'une fonction d'événement Lambda rencontre une erreur irrécupérable, votre client Amazon MQ arrête de traiter les enregistrements. D'autres consommateurs peuvent continuer le traitement, à condition qu'ils ne rencontrent pas la même erreur. Pour déterminer la cause potentielle d'un consommateur arrêté, vérifiez le champ `StateTransitionReason` dans les détails de retour de votre `EventSourceMapping` pour l'un des codes suivants :

`ESM_CONFIG_NOT_VALID`

La configuration de mappage de source d'événement n'est pas valide.

`EVENT_SOURCE_AUTHN_ERROR`

Lambda n'a pas réussi à authentifier la source de l'événement.

`EVENT_SOURCE_AUTHZ_ERROR`

Lambda ne dispose pas des autorisations requises pour accéder à la source d'événement.

`FUNCTION_CONFIG_NOT_VALID`

La configuration de la fonction n'est pas valide.

Les enregistrements ne sont pas non plus traités si Lambda les abandonne en raison de leur taille. La taille limite pour les enregistrements Lambda est de 6 Mo. Pour relivrer des messages en cas d'erreur de fonction, vous pouvez utiliser une file d'attente de lettres mortes (DLQ). Pour plus d'informations, consultez Message Redelivery and DLQ Handling (Relivraison des messages et gestion des DLQ), et le Guide de fiabilité sur le site web RabbitMQ.

> **Note**
>
> Lambda ne prend pas en charge les stratégies de relivraison personnalisées. Au lieu de cela, Lambda utilise une stratégie avec les valeurs par défaut de la page Stratégie de relivraison sur le site web d'Apache ActiveMQ, avec `maximumRedeliveries` défini sur 6.

Utilisation AWS Lambda avec Amazon RDS

Vous pouvez connecter une fonction d'événement Lambda à une base de données Amazon Relational Database Service (Amazon RDS) directement et via un proxy Amazon RDS. Les connexions directes sont utiles dans les scénarios simples, et les proxys sont recommandés pour la production. Un proxy de base de données gère un groupe de connexions partagées à la base de données qui permet à votre fonction d'atteindre des niveaux de simultanéité élevés sans épuiser les connexions de base de données.

Pour déterminer s'il convient d'utiliser Amazon RDS ou DynamoDB pour votre charge de travail, consultez. the section called “Amazon RDS et DynamoDB”

Nous vous recommandons d'utiliser le proxy Amazon RDS pour les fonctions d'événement Lambda qui établissent fréquemment de courtes connexions à la base de données ou qui ouvrent et ferment un grand nombre de connexions à la base de données. Pour de plus amples informations, veuillez consulter la rubrique Automatically connecting a Lambda function and a DB instance du Guide du développeur Amazon Relational Database Service.

> **Tip**
>
> Pour connecter rapidement une fonction d'événement Lambda à une base de données Amazon RDS, vous pouvez utiliser l'assistant guidé intégré à la console. Procédez comme suit pour ouvrir l'assistant :
>
> 1. Ouvrez la page Event Functions de la console Lambda.
> 2. Sélectionnez la fonction à laquelle vous souhaitez connecter une base de données.
> 3. Dans l'onglet Configuration, sélectionnez Bases de données RDS.
> 4. Choisissez Se connecter à la base de données RDS.
>
> Après avoir connecté votre fonction à une base de données, vous pouvez créer un proxy en choisissant Ajouter un proxy.

Configuration de votre fonction d'événement pour qu'elle fonctionne avec les ressources RDS

Dans la console Lambda, vous pouvez allouer et configurer des instances de base de données et des ressources de proxy Amazon RDS. Vous pouvez le faire en accédant aux Bases de données

RDS sous l'onglet Configuration. Vous pouvez également créer et configurer des connexions à Lambda Event Functions dans la console Amazon RDS. Lorsque vous configurez une instance de base de données RDS à utiliser avec Lambda, tenez compte des critères suivants :

- Pour se connecter à une base de données, votre fonction doit résider dans le même Amazon VPC où votre base de données s'exécute.
- Vous pouvez utiliser les bases de données Amazon RDS avec les moteurs MySQL, MariaDB, PostgreSQL ou Microsoft SQL Server.
- Vous pouvez également utiliser des clusters de base de données Aurora avec des moteurs MySQL ou PostgreSQL.
- Vous devez fournir un secret Secrets Manager pour l'authentification de la base de données.
- Un rôle IAM doit autoriser l'utilisation du secret et une stratégie d'approbation doit autoriser Amazon RDS à endosser le rôle.
- Le principal IAM qui utilise la console pour configurer la ressource Amazon RDS et la connecter à votre fonction doit disposer des autorisations suivantes :

Exemple de politique d'autorisations

> **Note**
>
> Vous n'avez besoin des autorisations de Proxy Amazon RDS que si vous configurez un Proxy Amazon RDS pour gérer un pool de connexions à votre base de données.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:AuthorizeSecurityGroupIngress",
```

```
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "rds-db:connect",
        "rds:CreateDBProxy",
        "rds:CreateDBInstance",
        "rds:CreateDBSubnetGroup",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstances",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyTargets",
        "rds:DescribeDBProxyTargetGroups",
        "rds:RegisterDBProxyTargets",
        "rds:ModifyDBInstance",
        "rds:ModifyDBProxy"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "lambda:CreateFunction",
        "lambda:ListFunctions",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:CreateRole",
        "iam:CreatePolicy"
      ],
      "Resource": "*"
```

```
    },
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:CreateSecret"
      ],
      "Resource": "*"
    }
  ]
}
```

Amazon RDS facture un tarif horaire pour les proxys en fonction de la taille de l'instance de base de données. Consultez la tarification des proxys RDS pour plus de détails. Pour plus d'informations sur les connexions de proxy en général, consultez Utilisation de Proxy Amazon RDS dans le Guide de l'utilisateur Amazon RDS.

SSL/TLS exigences relatives aux connexions Amazon RDS

Pour établir des SSL/TLS connexions sécurisées à une instance de base de données Amazon RDS, votre fonction d'événement Lambda doit vérifier l'identité du serveur de base de données à l'aide d'un certificat sécurisé. Lambda gère ces certificats différemment selon le type de package de déploiement :

- Archives .zip : la gestion des certificats varie en fonction de l'environnement d'exécution :
  - Node.js 18 et versions antérieures : Lambda inclut automatiquement les certificats CA et RDS.
  - Node.js 20 et versions ultérieures : Lambda ne charge plus de certificats CA supplémentaires par défaut. Définissez la variable d'environnement `NODE_EXTRA_CA_CERTS` sur `/var/runtime/ca-cert.pem`.

  L'ajout de nouveaux certificats Amazon RDS aux environnements d'exécution gérés par Lambda peut Régions AWS prendre jusqu'à 4 semaines.
- Images de conteneur : les images AWS de base incluent uniquement les certificats CA. Si votre fonction se connecte à une instance de base de données Amazon RDS, vous devez inclure les certificats appropriés dans votre image de conteneur. Dans votre Dockerfile, téléchargez le bundle

de certificats correspondant à l' Région AWS endroit où vous hébergez votre base de données. Exemple :

```
RUN curl https://truststore.pki.rds.amazonaws.com/us-east-1/us-east-1-bundle.pem -o /
us-east-1-bundle.pem
```

Cette commande télécharge le bundle de certificats Amazon RDS et l'enregistre sur le chemin absolu `/us-east-1-bundle.pem` dans le répertoire racine de votre conteneur. Lorsque vous configurez la connexion à la base de données dans le code de votre fonction, vous devez référencer ce chemin exact. Exemple :

Node.js

Cette `readFileSync` fonction est requise car les clients Node.js de base de données ont besoin du contenu réel du certificat en mémoire, et pas seulement du chemin d'accès au fichier de certificat. Sans `readFileSync`, le client interprète la chaîne de chemin comme le contenu du certificat, ce qui entraîne une erreur « certificat autosigné dans la chaîne de certificats ».

Example Node.js configuration de connexion pour la fonction OCI

```
import { readFileSync } from 'fs';

// ...

let connectionConfig = {
    host: process.env.ProxyHostName,
    user: process.env.DBUserName,
    password: token,
    database: process.env.DBName,
    ssl: {
        ca: readFileSync('/us-east-1-bundle.pem') // Load RDS certificate content
 from file into memory
    }
};
```

Python

Example Configuration de la connexion pour la fonction OCI Python

```
connection = pymysql.connect(
```

```
    host=proxy_host_name,
    user=db_username,
    password=token,
    db=db_name,
    port=port,
    ssl={'ca': '/us-east-1-bundle.pem'}  #Path to the certificate in container
)
```

Java

Pour les fonctions Java utilisant des connexions JDBC, la chaîne de connexion doit inclure :

- `useSSL=true`
- `requireSSL=true`
- Paramètre `sslCA` indiquant l'emplacement du certificat Amazon RDS dans l'image de conteneur

Example Chaîne de connexion pour la fonction OCI Java

```
// Define connection string
String connectionString = String.format("jdbc:mysql://%s:%s/%s?
useSSL=true&requireSSL=true&sslCA=/us-east-1-bundle.pem", // Path to the certificate
 in container
        System.getenv("ProxyHostName"),
        System.getenv("Port"),
        System.getenv("DBName"));
```

.NET

Example Chaîne de connexion pour la connexion MySQL dans la fonction OCI .NET

```
/// Build the Connection String with the Token
string connectionString =
 $"Server={Environment.GetEnvironmentVariable("RDS_ENDPOINT")};" +
                         $"Port={Environment.GetEnvironmentVariable("RDS_PORT")};" +

 $"Uid={Environment.GetEnvironmentVariable("RDS_USERNAME")};" +
                         $"Pwd={authToken};" +
                         "SslMode=Required;" +
                         "SslCa=/us-east-1-bundle.pem";  // Path to the certificate
 in container
```

Go

Pour les fonctions Go utilisant des connexions MySQL, chargez le certificat Amazon RDS dans un groupe de certificats et enregistrez-le avec le pilote MySQL. La chaîne de connexion doit ensuite référencer cette configuration à l'aide du paramètre `tls`.

Example Code Go pour la connexion MySQL dans la fonction OCI

```
import (
    "crypto/tls"
    "crypto/x509"
    "os"
    "github.com/go-sql-driver/mysql"
)

...

// Create certificate pool and register TLS config
rootCertPool := x509.NewCertPool()
pem, err := os.ReadFile("/us-east-1-bundle.pem")  // Path to the certificate in
 container
if err != nil {
    panic("failed to read certificate file: " + err.Error())
}
if ok := rootCertPool.AppendCertsFromPEM(pem); !ok {
    panic("failed to append PEM")
}

mysql.RegisterTLSConfig("custom", &tls.Config{
    RootCAs: rootCertPool,
})

dsn := fmt.Sprintf("%s:%s@tcp(%s)/%s?allowCleartextPasswords=true&tls=custom",
    dbUser, authenticationToken, dbEndpoint, dbName,
)
```

Ruby

Example Configuration de connexion Ruby pour la fonction OCI

```
conn = Mysql2::Client.new(
    host: endpoint,
    username: user,
```

```
    password: token,
    port: port,
    database: db_name,
    sslca: '/us-east-1-bundle.pem',  # Path to the certificate in container
    sslverify: true
)
```

Connexion à une base de données Amazon RDS dans une fonction d'événement Lambda

Les exemples de code suivants montrent comment implémenter une fonction d'événement Lambda qui se connecte à une base de données Amazon RDS. La fonction effectue une simple requête de base de données et renvoie le résultat.

> **Note**
>
> Ces exemples de code ne sont valides que pour les packages de déploiement .zip. Si vous déployez votre fonction à l'aide d'une image de conteneur, vous devez spécifier le fichier de certificat Amazon RDS dans le code de votre fonction, comme expliqué dans la section précédente.

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Connexion à une base de données Amazon RDS dans une fonction Lambda à l'aide de .NET.

```
using System.Data;
using System.Text.Json;
using Amazon.Lambda.APIGatewayEvents;
using Amazon.Lambda.Core;
using MySql.Data.MySqlClient;
```

```
// Assembly attribute to enable the Lambda function's JSON input to be converted
 into a .NET class.
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSeri

namespace aws_rds;

public class InputModel
{
    public string key1 { get; set; }
    public string key2 { get; set; }
}

public class Function
{
    /// <summary>
    // Handles the Lambda function execution for connecting to RDS using IAM
 authentication.
    /// </summary>
    /// <param name="input">The input event data passed to the Lambda function</
param>
    /// <param name="context">The Lambda execution context that provides runtime
 information</param>
    /// <returns>A response object containing the execution result</returns>

    public async Task<APIGatewayProxyResponse>
 FunctionHandler(APIGatewayProxyRequest request, ILambdaContext context)
    {
        // Sample Input: {"body": "{\"key1\":\"20\", \"key2\":\"25\"}"}
        var input = JsonSerializer.Deserialize<InputModel>(request.Body);

        /// Obtain authentication token
        var authToken = RDSAuthTokenGenerator.GenerateAuthToken(
            Environment.GetEnvironmentVariable("RDS_ENDPOINT"),
            Convert.ToInt32(Environment.GetEnvironmentVariable("RDS_PORT")),
            Environment.GetEnvironmentVariable("RDS_USERNAME")
        );

        /// Build the Connection String with the Token
        string connectionString =
 $"Server={Environment.GetEnvironmentVariable("RDS_ENDPOINT")};" +

 $"Port={Environment.GetEnvironmentVariable("RDS_PORT")};" +
```

```
$"Uid={Environment.GetEnvironmentVariable("RDS_USERNAME")};" +
                                  $"Pwd={authToken};";


       try
       {
           await using var connection = new MySqlConnection(connectionString);
           await connection.OpenAsync();

           const string sql = "SELECT @param1 + @param2 AS Sum";

           await using var command = new MySqlCommand(sql, connection);
           command.Parameters.AddWithValue("@param1", int.Parse(input.key1 ??
"0"));
           command.Parameters.AddWithValue("@param2", int.Parse(input.key2 ??
"0"));

           await using var reader = await command.ExecuteReaderAsync();
           if (await reader.ReadAsync())
           {
               int result = reader.GetInt32("Sum");

               //Sample Response: {"statusCode":200,"body":"{\"message\":\"The
sum is: 45\"}","isBase64Encoded":false}
               return new APIGatewayProxyResponse
               {
                   StatusCode = 200,
                   Body = JsonSerializer.Serialize(new { message = $"The sum is:
{result}" })
               };
           }

       }
       catch (Exception ex)
       {
           Console.WriteLine($"Error: {ex.Message}");
       }

       return new APIGatewayProxyResponse
       {
           StatusCode = 500,
           Body = JsonSerializer.Serialize(new { error = "Internal server
error" })
```

```
        };
    }
}
```

Go

Kit SDK pour Go V2

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Connexion à une base de données Amazon RDS dans une fonction Lambda à l'aide de Go.

```
/*
Golang v2 code here.
*/

package main

import (
 "context"
 "database/sql"
 "encoding/json"
 "fmt"
 "os"

 "github.com/aws/aws-lambda-go/lambda"
 "github.com/aws/aws-sdk-go-v2/config"
 "github.com/aws/aws-sdk-go-v2/feature/rds/auth"
 _ "github.com/go-sql-driver/mysql"
)

type MyEvent struct {
 Name string `json:"name"`
}

func HandleRequest(event *MyEvent) (map[string]interface{}, error) {
```

```
var dbName string = os.Getenv("DatabaseName")
var dbUser string = os.Getenv("DatabaseUser")
var dbHost string = os.Getenv("DBHost") // Add hostname without https
var dbPort int = os.Getenv("Port")      // Add port number
var dbEndpoint string = fmt.Sprintf("%s:%d", dbHost, dbPort)
var region string = os.Getenv("AWS_REGION")

cfg, err := config.LoadDefaultConfig(context.TODO())
if err != nil {
 panic("configuration error: " + err.Error())
}

authenticationToken, err := auth.BuildAuthToken(
 context.TODO(), dbEndpoint, region, dbUser, cfg.Credentials)
if err != nil {
 panic("failed to create authentication token: " + err.Error())
}

dsn := fmt.Sprintf("%s:%s@tcp(%s)/%s?tls=true&allowCleartextPasswords=true",
 dbUser, authenticationToken, dbEndpoint, dbName,
)

db, err := sql.Open("mysql", dsn)
if err != nil {
 panic(err)
}

defer db.Close()

var sum int
err = db.QueryRow("SELECT ?+? AS sum", 3, 2).Scan(&sum)
if err != nil {
 panic(err)
}
s := fmt.Sprint(sum)
message := fmt.Sprintf("The selected sum is: %s", s)

messageBytes, err := json.Marshal(message)
if err != nil {
 return nil, err
}

messageString := string(messageBytes)
return map[string]interface{}{
```

```
  "statusCode": 200,
  "headers":    map[string]string{"Content-Type": "application/json"},
  "body":       messageString,
 }, nil
}

func main() {
 lambda.Start(HandleRequest)
}
```

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Connexion à une base de données Amazon RDS dans une fonction Lambda à l'aide de Java.

```
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.APIGatewayProxyRequestEvent;
import com.amazonaws.services.lambda.runtime.events.APIGatewayProxyResponseEvent;
import software.amazon.awssdk.auth.credentials.DefaultCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.rdsdata.RdsDataClient;
import software.amazon.awssdk.services.rdsdata.model.ExecuteStatementRequest;
import software.amazon.awssdk.services.rdsdata.model.ExecuteStatementResponse;
import software.amazon.awssdk.services.rdsdata.model.Field;

import java.sql.Connection;
import java.sql.DriverManager;
import java.sql.PreparedStatement;
import java.sql.ResultSet;

public class RdsLambdaHandler implements
 RequestHandler<APIGatewayProxyRequestEvent, APIGatewayProxyResponseEvent> {
```

```
    @Override
    public APIGatewayProxyResponseEvent handleRequest(APIGatewayProxyRequestEvent
 event, Context context) {
        APIGatewayProxyResponseEvent response = new
 APIGatewayProxyResponseEvent();

        try {
            // Obtain auth token
            String token = createAuthToken();

            // Define connection configuration
            String connectionString = String.format("jdbc:mysql://%s:%s/%s?
useSSL=true&requireSSL=true",
                    System.getenv("ProxyHostName"),
                    System.getenv("Port"),
                    System.getenv("DBName"));

            // Establish a connection to the database
            try (Connection connection =
 DriverManager.getConnection(connectionString, System.getenv("DBUserName"),
 token);
                 PreparedStatement statement =
 connection.prepareStatement("SELECT ? + ? AS sum")) {

                statement.setInt(1, 3);
                statement.setInt(2, 2);

                try (ResultSet resultSet = statement.executeQuery()) {
                    if (resultSet.next()) {
                        int sum = resultSet.getInt("sum");
                        response.setStatusCode(200);
                        response.setBody("The selected sum is: " + sum);
                    }
                }
            }

        } catch (Exception e) {
            response.setStatusCode(500);
            response.setBody("Error: " + e.getMessage());
        }

        return response;
    }
```

```
    private String createAuthToken() {
        // Create RDS Data Service client
        RdsDataClient rdsDataClient = RdsDataClient.builder()
                .region(Region.of(System.getenv("AWS_REGION")))
                .credentialsProvider(DefaultCredentialsProvider.create())
                .build();

        // Define authentication request
        ExecuteStatementRequest request = ExecuteStatementRequest.builder()
                .resourceArn(System.getenv("ProxyHostName"))
                .secretArn(System.getenv("DBUserName"))
                .database(System.getenv("DBName"))
                .sql("SELECT 'RDS IAM Authentication'")
                .build();

        // Execute request and obtain authentication token
        ExecuteStatementResponse response =
 rdsDataClient.executeStatement(request);
        Field tokenField = response.records().get(0).get(0);

        return tokenField.stringValue();
    }
}
```

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Connexion à une base de données Amazon RDS dans une fonction Lambda à l'aide de. JavaScript

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
/*
```

```
Node.js code here.
*/
// ES6+ example
import { Signer } from "@aws-sdk/rds-signer";
import mysql from 'mysql2/promise';

async function createAuthToken() {
  // Define connection authentication parameters
  const dbinfo = {

    hostname: process.env.ProxyHostName,
    port: process.env.Port,
    username: process.env.DBUserName,
    region: process.env.AWS_REGION,

  }

  // Create RDS Signer object
  const signer = new Signer(dbinfo);

  // Request authorization token from RDS, specifying the username
  const token = await signer.getAuthToken();
  return token;
}

async function dbOps() {

  // Obtain auth token
  const token = await createAuthToken();
  // Define connection configuration
  let connectionConfig = {
    host: process.env.ProxyHostName,
    user: process.env.DBUserName,
    password: token,
    database: process.env.DBName,
    ssl: 'Amazon RDS'
  }
  // Create the connection to the DB
  const conn = await mysql.createConnection(connectionConfig);
  // Obtain the result of the query
  const [res,] = await conn.execute('select ?+? as sum', [3, 2]);
  return res;

}
```

```
export const handler = async (event) => {
  // Execute database flow
  const result = await dbOps();
  // Return result
  return {
    statusCode: 200,
    body: JSON.stringify("The selected sum is: " + result[0].sum)
  }
};
```

Connexion à une base de données Amazon RDS dans une fonction Lambda à l'aide de. TypeScript

```
import { Signer } from "@aws-sdk/rds-signer";
import mysql from 'mysql2/promise';

// RDS settings
// Using '!' (non-null assertion operator) to tell the TypeScript compiler that
 the DB settings are not null or undefined,
const proxy_host_name = process.env.PROXY_HOST_NAME!
const port = parseInt(process.env.PORT!)
const db_name = process.env.DB_NAME!
const db_user_name = process.env.DB_USER_NAME!
const aws_region = process.env.AWS_REGION!


async function createAuthToken(): Promise<string> {

    // Create RDS Signer object
    const signer = new Signer({
        hostname: proxy_host_name,
        port: port,
        region: aws_region,
        username: db_user_name
    });

    // Request authorization token from RDS, specifying the username
    const token = await signer.getAuthToken();
    return token;
}
```

```
async function dbOps(): Promise<mysql.QueryResult | undefined> {
    try {
        // Obtain auth token
        const token = await createAuthToken();
        const conn = await mysql.createConnection({
            host: proxy_host_name,
            user: db_user_name,
            password: token,
            database: db_name,
            ssl: 'Amazon RDS' // Ensure you have the CA bundle for SSL connection
        });
        const [rows, fields] = await conn.execute('SELECT ? + ? AS sum', [3, 2]);
        console.log('result:', rows);
        return rows;
    }
    catch (err) {
        console.log(err);
    }
}

export const lambdaHandler = async (event: any): Promise<{ statusCode: number;
 body: string }> => {
    // Execute database flow
    const result = await dbOps();

    // Return error is result is undefined
    if (result == undefined)
        return {
            statusCode: 500,
            body: JSON.stringify(`Error with connection to DB host`)
        }

    // Return result
    return {
        statusCode: 200,
        body: JSON.stringify(`The selected sum is: ${result[0].sum}`)
    };
};
```

PHP

Kit SDK pour PHP

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Connexion à une base de données Amazon RDS dans une fonction Lambda à l'aide de PHP.

```
<?php
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0

# using bref/bref and bref/logger for simplicity

use Bref\Context\Context;
use Bref\Event\Handler as StdHandler;
use Bref\Logger\StderrLogger;
use Aws\Rds\AuthTokenGenerator;
use Aws\Credentials\CredentialProvider;

require __DIR__ . '/vendor/autoload.php';

class Handler implements StdHandler
{
    private StderrLogger $logger;
    public function __construct(StderrLogger $logger)
    {
        $this->logger = $logger;
    }


    private function getAuthToken(): string {
        // Define connection authentication parameters
        $dbConnection = [
            'hostname' => getenv('DB_HOSTNAME'),
            'port' => getenv('DB_PORT'),
            'username' => getenv('DB_USERNAME'),
            'region' => getenv('AWS_REGION'),
        ];
```

```
        // Create RDS AuthTokenGenerator object
        $generator = new
AuthTokenGenerator(CredentialProvider::defaultProvider());

        // Request authorization token from RDS, specifying the username
        return $generator->createToken(
            $dbConnection['hostname'] . ':' . $dbConnection['port'],
            $dbConnection['region'],
            $dbConnection['username']
        );
    }

    private function getQueryResults() {
        // Obtain auth token
        $token = $this->getAuthToken();

        // Define connection configuration
        $connectionConfig = [
            'host' => getenv('DB_HOSTNAME'),
            'user' => getenv('DB_USERNAME'),
            'password' => $token,
            'database' => getenv('DB_NAME'),
        ];

        // Create the connection to the DB
        $conn = new PDO(

"mysql:host={$connectionConfig['host']};dbname={$connectionConfig['database']}",
            $connectionConfig['user'],
            $connectionConfig['password'],
            [
                PDO::MYSQL_ATTR_SSL_CA => '/path/to/rds-ca-2019-root.pem',
                PDO::MYSQL_ATTR_SSL_VERIFY_SERVER_CERT => true,
            ]
        );

        // Obtain the result of the query
        $stmt = $conn->prepare('SELECT ?+? AS sum');
        $stmt->execute([3, 2]);

        return $stmt->fetch(PDO::FETCH_ASSOC);
    }
```

```
    /**
     * @param mixed $event
     * @param Context $context
     * @return array
     */
    public function handle(mixed $event, Context $context): array
    {
        $this->logger->info("Processing query");

        // Execute database flow
        $result = $this->getQueryResults();

        return [
            'sum' => $result['sum']
        ];
    }
}

$logger = new StderrLogger();
return new Handler($logger);
```

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Connexion à une base de données Amazon RDS dans une fonction Lambda à l'aide de Python.

```
import json
import os
import boto3
import pymysql

# RDS settings
proxy_host_name = os.environ['PROXY_HOST_NAME']
```

```
port = int(os.environ['PORT'])
db_name = os.environ['DB_NAME']
db_user_name = os.environ['DB_USER_NAME']
aws_region = os.environ['AWS_REGION']


# Fetch RDS Auth Token
def get_auth_token():
    client = boto3.client('rds')
    token = client.generate_db_auth_token(
        DBHostname=proxy_host_name,
        Port=port
        DBUsername=db_user_name
        Region=aws_region
    )
    return token

def lambda_handler(event, context):
    token = get_auth_token()
    try:
        connection = pymysql.connect(
            host=proxy_host_name,
            user=db_user_name,
            password=token,
            db=db_name,
            port=port,
            ssl={'ca': 'Amazon RDS'}  # Ensure you have the CA bundle for SSL
 connection
        )

        with connection.cursor() as cursor:
            cursor.execute('SELECT %s + %s AS sum', (3, 2))
            result = cursor.fetchone()

        return result

    except Exception as e:
        return (f"Error: {str(e)}")  # Return an error message if an exception
 occurs
```

Ruby

Kit SDK pour Ruby

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Connexion à une base de données Amazon RDS dans une fonction Lambda à l'aide de Ruby.

```
# Ruby code here.

require 'aws-sdk-rds'
require 'json'
require 'mysql2'

def lambda_handler(event:, context:)
  endpoint = ENV['DBEndpoint'] # Add the endpoint without https"
  port = ENV['Port']           # 3306
  user = ENV['DBUser']
  region = ENV['DBRegion']     # 'us-east-1'
  db_name = ENV['DBName']

  credentials = Aws::Credentials.new(
    ENV['AWS_ACCESS_KEY_ID'],
    ENV['AWS_SECRET_ACCESS_KEY'],
    ENV['AWS_SESSION_TOKEN']
  )
  rds_client = Aws::RDS::AuthTokenGenerator.new(
    region: region,
    credentials: credentials
  )

  token = rds_client.auth_token(
    endpoint: endpoint+ ':' + port,
    user_name: user,
    region: region
  )

  begin
    conn = Mysql2::Client.new(
```

```
      host: endpoint,
      username: user,
      password: token,
      port: port,
      database: db_name,
      sslca: '/var/task/global-bundle.pem',
      sslverify: true,
      enable_cleartext_plugin: true
    )
    a = 3
    b = 2
    result = conn.query("SELECT #{a} + #{b} AS sum").first['sum']
    puts result
    conn.close
    {
      statusCode: 200,
      body: result.to_json
    }
  rescue => e
    puts "Database connection failed due to #{e}"
  end
end
```

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Connexion à une base de données Amazon RDS dans une fonction Lambda à l'aide de Rust.

```
use aws_config::BehaviorVersion;
use aws_credential_types::provider::ProvideCredentials;
use aws_sigv4::{
    http_request::{sign, SignableBody, SignableRequest, SigningSettings},
    sign::v4,
};
use lambda_runtime::{run, service_fn, Error, LambdaEvent};
```

```
use serde_json::{json, Value};
use sqlx::postgres::PgConnectOptions;
use std::env;
use std::time::{Duration, SystemTime};

const RDS_CERTS: &[u8] = include_bytes!("global-bundle.pem");

async fn generate_rds_iam_token(
    db_hostname: &str,
    port: u16,
    db_username: &str,
) -> Result<String, Error> {
    let config = aws_config::load_defaults(BehaviorVersion::v2024_03_28()).await;

    let credentials = config
        .credentials_provider()
        .expect("no credentials provider found")
        .provide_credentials()
        .await
        .expect("unable to load credentials");
    let identity = credentials.into();
    let region = config.region().unwrap().to_string();

    let mut signing_settings = SigningSettings::default();
    signing_settings.expires_in = Some(Duration::from_secs(900));
    signing_settings.signature_location =
 aws_sigv4::http_request::SignatureLocation::QueryParams;

    let signing_params = v4::SigningParams::builder()
        .identity(&identity)
        .region(&region)
        .name("rds-db")
        .time(SystemTime::now())
        .settings(signing_settings)
        .build()?;

    let url = format!(
        "https://{db_hostname}:{port}/?Action=connect&DBUser={db_user}",
        db_hostname = db_hostname,
        port = port,
        db_user = db_username
    );

    let signable_request =
```

```
        SignableRequest::new("GET", &url, std::iter::empty(),
 SignableBody::Bytes(&[]))
            .expect("signable request");

    let (signing_instructions, _signature) =
        sign(signable_request, &signing_params.into())?.into_parts();

    let mut url = url::Url::parse(&url).unwrap();
    for (name, value) in signing_instructions.params() {
        url.query_pairs_mut().append_pair(name, &value);
    }

    let response = url.to_string().split_off("https://".len());

    Ok(response)
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    run(service_fn(handler)).await
}

async fn handler(_event: LambdaEvent<Value>) -> Result<Value, Error> {
    let db_host = env::var("DB_HOSTNAME").expect("DB_HOSTNAME must be set");
    let db_port = env::var("DB_PORT")
        .expect("DB_PORT must be set")
        .parse::<u16>()
        .expect("PORT must be a valid number");
    let db_name = env::var("DB_NAME").expect("DB_NAME must be set");
    let db_user_name = env::var("DB_USERNAME").expect("DB_USERNAME must be set");

    let token = generate_rds_iam_token(&db_host, db_port, &db_user_name).await?;

    let opts = PgConnectOptions::new()
        .host(&db_host)
        .port(db_port)
        .username(&db_user_name)
        .password(&token)
        .database(&db_name)
        .ssl_root_cert_from_pem(RDS_CERTS.to_vec())
        .ssl_mode(sqlx::postgres::PgSslMode::Require);

    let pool = sqlx::postgres::PgPoolOptions::new()
        .connect_with(opts)
```

```
        .await?;

    let result: i32 = sqlx::query_scalar("SELECT $1 + $2")
        .bind(3)
        .bind(2)
        .fetch_one(&pool)
        .await?;

    println!("Result: {:?}", result);

    Ok(json!({
        "statusCode": 200,
        "content-type": "text/plain",
        "body": format!("The selected sum is: {result}")
    }))
}
```

Traitement des notifications d'événements provenant d'Amazon RDS

Vous pouvez utiliser Lambda pour traiter les notifications d'événements d'une base de données Amazon RDS. Amazon RDS envoie des notifications à une rubrique Amazon Simple Notification Service (Amazon SNS), que vous pouvez configurer pour appeler une fonction d'événement Lambda. Amazon SNS enveloppe le message d'Amazon RDS dans son propre document d'événement, et l'envoie à votre fonction.

Pour plus d'informations sur la configuration d'une base de données Amazon RDS pour envoyer des notifications, consultez Utilisation des notifications d'événements Amazon RDS.

Example Message Amazon RDS dans un événement Amazon SNS

```
{
        "Records": [
          {
            "EventVersion": "1.0",
            "EventSubscriptionArn": "arn:aws:sns:us-east-2:123456789012:rds-
lambda:21be56ed-a058-49f5-8c98-aedd2564c486",
            "EventSource": "aws:sns",
            "Sns": {
              "SignatureVersion": "1",
              "Timestamp": "2023-01-02T12:45:07.000Z",
```

```
              "Signature": "tcc6faL2yUC6dgZdmrwh1Y4cGa/ebXEkAi6RibDsvpi
+tE/1+82j...65r==",
              "SigningCertUrl": "https://sns.us-east-2.amazonaws.com/
SimpleNotificationService-ac565b8b1a6c5d002d285f9598aa1d9b.pem",
              "MessageId": "95df01b4-ee98-5cb9-9903-4c221d41eb5e",
              "Message": "{\"Event Source\":\"db-instance\",\"Event Time\":\"2023-01-02
 12:45:06.000\",\"Identifier Link\":\"https://console.aws.amazon.com/rds/home?
region=eu-west-1#dbinstance:id=dbinstanceid\",\"Source ID\":\"dbinstanceid\",\"Event ID
\":\"http://docs.amazonwebservices.com/AmazonRDS/latest/UserGuide/USER_Events.html#RDS-
EVENT-0002\",\"Event Message\":\"Finished DB Instance backup\"}",
              "MessageAttributes": {},
              "Type": "Notification",
              "UnsubscribeUrl": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&amp;SubscriptionArn=arn:aws:sns:us-east-2:123456789012:test-
lambda:21be56ed-a058-49f5-8c98-aedd2564c486",
              "TopicArn":"arn:aws:sns:us-east-2:123456789012:sns-lambda",
              "Subject": "RDS Notification Message"
            }
          }
        ]
      }
```

Tutoriel complet Lambda et Amazon RDS

- Utilisation d'une fonction Lambda pour accéder à une base de données Amazon RDS — Dans le guide de l'utilisateur Amazon RDS, découvrez comment utiliser une fonction d'événement Lambda pour écrire des données dans une base de données Amazon RDS via un proxy Amazon RDS. Votre fonction d'événement Lambda lit les enregistrements d'une file d'attente Amazon SQS et écrit de nouveaux éléments dans une table de votre base de données chaque fois qu'un message est ajouté.

Sélectionnez un service de base de données pour vos Lambda-based applications

De nombreuses applications sans serveur ont besoin de stocker et de récupérer des données. AWS propose plusieurs options de base de données qui fonctionnent avec les fonctions d'événement Lambda. Les deux options les plus populaires sont Amazon DynamoDB, un service de base de données NoSQL, et Amazon RDS, une solution de base de données relationnelle traditionnelle. Les sections suivantes expliquent les principales différences entre ces services lorsque vous les utilisez avec Lambda, et vous aident à sélectionner le service de base de données adapté à votre application sans serveur.

Pour en savoir plus sur les autres services de base de données proposés par AWS, et pour comprendre leurs cas d'utilisation et leurs inconvénients de manière plus générale, voir Choisir un service de AWS base de données. Tous les services de AWS base de données sont compatibles avec Lambda, mais ils ne sont peut-être pas tous adaptés à votre cas d'utilisation particulier.

Quelles sont les options proposées lors de la sélection d'un service de base de données avec Lambda ?

AWS propose plusieurs services de base de données. Pour les applications sans serveur, DynamoDB et Amazon RDS sont deux des options les plus populaires.

- DynamoDB est un service de base de données NoSQL entièrement géré, optimisé pour les applications sans serveur. Il offre une mise à l'échelle transparente et des performances constantes de l'ordre de quelques millisecondes à n'importe quelle échelle.
- Amazon RDS est un service de base de données relationnelle géré qui prend en charge plusieurs moteurs de base de données, dont MySQL et PostgreSQL. Il fournit les fonctionnalités familières de SQL avec une infrastructure gérée.

Recommandations si vous connaissez déjà vos besoins

Si vous connaissez déjà bien vos besoins, voici nos recommandations de base :

Nous recommandons DynamoDB pour les applications sans serveur qui ont besoin de performances constantes à faible latence et d'une mise à l'échelle automatique, et qui ne nécessitent pas de jointures ou de transactions complexes. Il est particulièrement bien adapté aux Lambda-based applications en raison de sa nature sans serveur.

Amazon RDS est un meilleur choix lorsque vous avez besoin de requêtes SQL complexes, de jointures ou si vous avez des applications existantes utilisant des bases de données relationnelles. Sachez toutefois que la connexion de Lambda Event Functions à Amazon RDS nécessite une configuration supplémentaire et peut avoir un impact sur les temps de démarrage à froid.

Éléments à prendre en compte lors de la sélection d'un service de base de données

Lorsque vous choisissez entre DynamoDB et Amazon RDS pour vos applications Lambda, tenez compte des facteurs suivants :

- Gestion des connexions et démarrages à froid
- Modèles d'accès aux données

- Complexité des requêtes
- Exigences de cohérence des données
- Caractéristiques de mise à l'échelle
- Modèle de coût

La compréhension de ces facteurs vous permettra de choisir l'option qui répond le mieux aux besoins de votre cas d'utilisation.

Gestion des connexions et démarrages à froid

- DynamoDB utilise une API HTTP pour toutes les opérations. Les fonctions d'événement Lambda peuvent effectuer des demandes immédiates sans maintenir les connexions, ce qui améliore les performances de démarrage à froid. Chaque demande est authentifiée à l'aide AWS d'informations d'identification sans surcoût de connexion.
- Amazon RDS nécessite de gérer des groupes de connexions, car il utilise des connexions de base de données traditionnelles. Cela peut affecter les démarrages à froid, car les nouvelles instances Lambda doivent établir des connexions. Vous devrez mettre en œuvre des stratégies de regroupement de connexions et éventuellement utiliser le Proxy Amazon RDS pour gérer efficacement les connexions. Notez que l'utilisation du Proxy Amazon RDS entraîne des coûts supplémentaires.

Modèles d'accès aux données

- DynamoDB fonctionne mieux avec les modèles d'accès connus et les modèles à table unique. Il est idéal pour les applications Lambda qui ont besoin d'un accès constant à faible latence aux données sur la base de clés primaires ou d'index secondaires.
- Amazon RDS offre de la flexibilité pour les requêtes complexes et les modèles d'accès changeants. Il est mieux adapté lorsque vos fonctions d'événement Lambda doivent effectuer des requêtes uniques et personnalisées ou des jointures complexes sur plusieurs tables.

Complexité des requêtes

- DynamoDB excelle dans les opérations simples basées sur les clés et dans les modèles d'accès prédéfinis. Les requêtes complexes doivent être conçues autour de structures d'index, et les jointures doivent être gérées dans le code de l'application.

- Amazon RDS prend en charge les requêtes SQL complexes avec des jointures, des sous-requêtes et des agrégations. Cela peut simplifier le code de votre fonction d'événement Lambda lorsque des opérations de données complexes sont nécessaires.

Exigences de cohérence des données

- DynamoDB propose à la fois des options de cohérence finale et de cohérence forte, la cohérence forte étant disponible pour les lectures d'un seul élément. Les transactions sont prises en charge, mais avec certaines restrictions.
- Amazon RDS offre une conformité totale en matière d'atomicité, de cohérence, d'isolation et de durabilité (ACID) et une prise en charge des transactions complexes. Si vos fonctions d'événement Lambda nécessitent des transactions complexes ou une forte cohérence entre plusieurs enregistrements, Amazon RDS peut être plus adapté.

Caractéristiques de mise à l'échelle

- DynamoDB s'adapte automatiquement à votre charge de travail. Il peut gérer les pics de trafic soudains provenant de Lambda Event Functions sans pré-provisionnement. Vous pouvez utiliser le mode de capacité à la demande pour ne payer que ce que vous utilisez, ce qui correspond parfaitement au modèle de mise à l'échelle de Lambda.
- Amazon RDS dispose d'une capacité fixe en fonction de la taille d'instance que vous choisissez. Si plusieurs fonctions d'événement Lambda tentent de se connecter simultanément, vous risquez de dépasser votre quota de connexion. Vous devez gérer avec soin les groupes de connexions et éventuellement implémenter une logique de nouvelle tentative.

Modèle de coût

- La tarification de DynamoDB est parfaitement adaptée aux applications sans serveur. Avec une capacité à la demande, vous ne payez que pour les lectures et écritures réellement effectuées par vos fonctions d'événement Lambda. Le temps d'inactivité n'est pas facturé.
- Amazon RDS facture l'instance en cours d'exécution, quelle que soit son utilisation. Cela peut être moins rentable pour les charges de travail sporadiques, qui sont courantes dans les applications sans serveur. Toutefois, cela peut s'avérer plus économique pour les charges de travail à haut débit avec une utilisation constante.

Commencer avec le service de base de données que vous avez choisi

Maintenant que vous avez pris connaissance des critères de sélection entre DynamoDB et Amazon RDS et des principales différences entre les deux, vous pouvez sélectionner l'option qui répond le mieux à vos besoins et utiliser les ressources suivantes pour commencer à l'utiliser.

DynamoDB

Mise en route avec DynamoDB grâce aux ressources suivantes

- Pour une présentation du service DynamoDB, consultez Qu'est-ce que DynamoDB ? dans le Guide du développeur Amazon DynamoDB
- Suivez le didacticiel Utilisation de Lambda avec API Gateway pour découvrir un exemple d'utilisation d'une fonction d'événement Lambda pour effectuer des opérations CRUD sur une table DynamoDB en réponse à une demande d'API.
- Consultez la section Programmation avec DynamoDB et AWS les kits SDK dans le guide du développeur Amazon DynamoDB pour en savoir plus sur la façon d'accéder à DynamoDB depuis votre fonction d'événement Lambda à l'aide de l'un des SDK. AWS

Amazon RDS

Mise en route avec Amazon RDS grâce aux ressources suivantes

- Pour une présentation du service Amazon RDS, consultez l'article Qu'est-ce que Amazon Relational Database Service (Amazon RDS) ? dans le Guide de l'utilisateur Amazon Relational Database Service.
- Suivez le didacticiel Utilisation d'une fonction Lambda pour accéder à une base de données Amazon RDS dans le Guide de l'utilisateur Amazon Relational Database Service.
- Pour en savoir plus sur l'utilisation de Lambda avec Amazon RDS, consultez the section called "RDS".

Traiter les notifications d’événements Amazon S3 avec Lambda

Vous pouvez utiliser Lambda pour traiter les notifications d’événement d’Amazon Simple Storage Service. Amazon S3 peut envoyer un événement à une fonction d'événement Lambda lorsqu'un objet est créé ou supprimé. Vous configurez des paramètres de notification sur un compartiment et accordez à Amazon S3 l’autorisation d’invoquer une fonction sur la stratégie d’autorisations basée sur une ressource de la fonction.

> **Warning**
>
> Si votre fonction d'événement Lambda utilise le même bucket qui la déclenche, elle peut s'exécuter en boucle. Par exemple, si le compartiment déclenche une fonction chaque fois qu’un objet est chargé et que la fonction charge un objet dans le compartiment, la fonction se déclenche elle-même indirectement. Afin d’éviter cela, utilisez deux compartiments ou configurez le déclencheur pour qu’il s’applique uniquement à un préfixe utilisé pour les objets entrants.

Amazon S3 appelle votre fonction de manière asynchrone avec un événement contenant des détails sur l’objet. L’exemple suivant montre un événement envoyé par Amazon S3 lors du chargement d’un package de déploiement vers Amazon S3.

Example Evénement de notification Amazon S3

```
{
  "Records": [
    {
      "eventVersion": "2.1",
      "eventSource": "aws:s3",
      "awsRegion": "us-east-2",
      "eventTime": "2019-09-03T19:37:27.192Z",
      "eventName": "ObjectCreated:Put",
      "userIdentity": {
        "principalId": "AWS:AIDAINPONIXQXHT3IKHL2"
      },
      "requestParameters": {
        "sourceIPAddress": "205.255.255.255"
      },
      "responseElements": {
        "x-amz-request-id": "D82B88E5F771F645",
```

```
        "x-amz-id-2":
 "vlR7PnpV2Ce81l0PRw6jlUpck7Jo5ZsQjryTjKlc5aLWGVHPZLj5NeC6qMa0emYBDXOo6QBU0Wo="
      },
      "s3": {
        "s3SchemaVersion": "1.0",
        "configurationId": "828aa6fc-f7b5-4305-8584-487c791949c1",
        "bucket": {
          "name": "amzn-s3-demo-bucket",
          "ownerIdentity": {
            "principalId": "A3I5XTEXAMAI3E"
          },
          "arn": "arn:aws:s3:::lambda-artifacts-deafc19498e3f2df"
        },
        "object": {
          "key": "b21b84d653bb07b05b1e6b33684dc11b",
          "size": 1305107,
          "eTag": "b21b84d653bb07b05b1e6b33684dc11b",
          "sequencer": "0C0F6F405D6ED209E1"
        }
      }
    }
  ]
}
```

Pour appeler votre fonction, Amazon S3 a besoin d'une autorisation de la stratégie basée sur une ressource. Lorsque vous configurez un déclencheur Amazon S3 dans la console Lambda, cette dernière modifie la stratégie basée sur une ressource pour permettre à Amazon S3 d'appeler la fonction si le nom du compartiment et l'ID de compte correspondent. Si vous configurez la notification dans Amazon S3, vous utilisez l'API Lambda pour mettre à jour la stratégie. Vous pouvez également utiliser l'API Lambda pour accorder une autorisation à un autre compte ou limiter l'autorisation à un alias désigné.

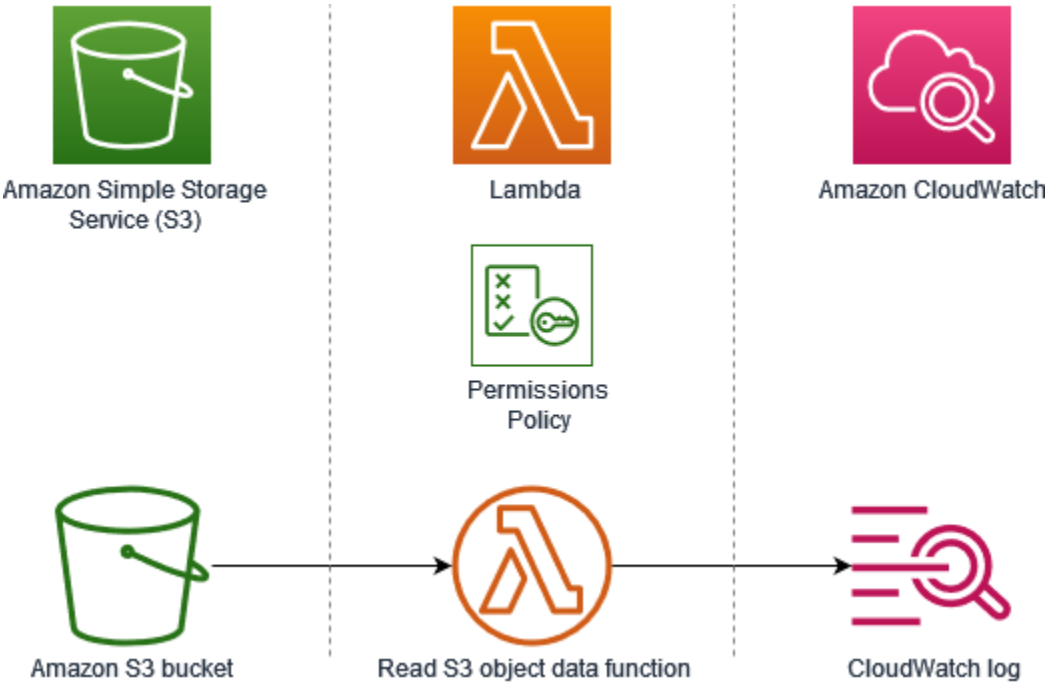
Si votre fonction utilise le AWS SDK pour gérer les ressources Amazon S3, elle a également besoin des autorisations Amazon S3 dans son rôle d'exécution.

Rubriques

- Tutoriel : Utilisation d'un déclencheur Amazon S3 pour appeler une fonction d'événement Lambda
- Didacticiel : Utilisation d'un déclencheur Amazon S3 pour créer des images miniatures

Tutoriel : Utilisation d'un déclencheur Amazon S3 pour appeler une fonction d'événement Lambda

Dans ce didacticiel, vous allez utiliser la console pour créer une fonction d'événement Lambda et configurer un déclencheur pour un bucket Amazon Simple Storage Service (Amazon S3). Chaque fois que vous ajoutez un objet à votre compartiment Amazon S3, votre fonction s'exécute et affiche le type d'objet dans Amazon CloudWatch Logs.

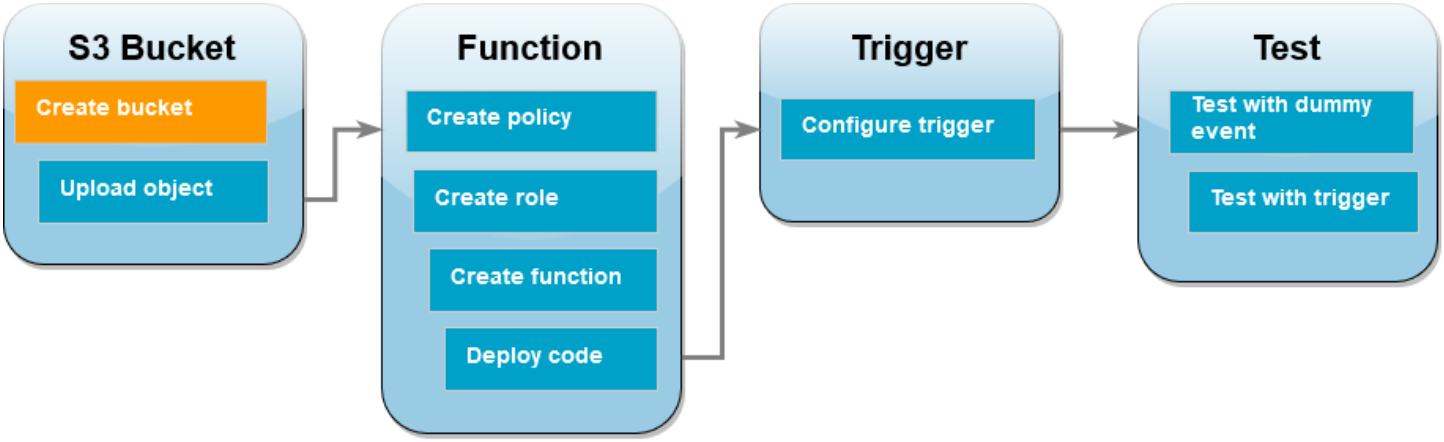


Ce tutoriel montre comment :

1. Créez un compartiment Amazon S3.
2. Créez une fonction d'événement Lambda qui renvoie le type d'objet des objets d'un compartiment Amazon S3.
3. Configurez un déclencheur Lambda qui invoque votre fonction lorsque des objets sont chargés dans votre compartiment.
4. Testez votre fonction, d’abord avec un événement fictif, puis en utilisant le déclencheur.

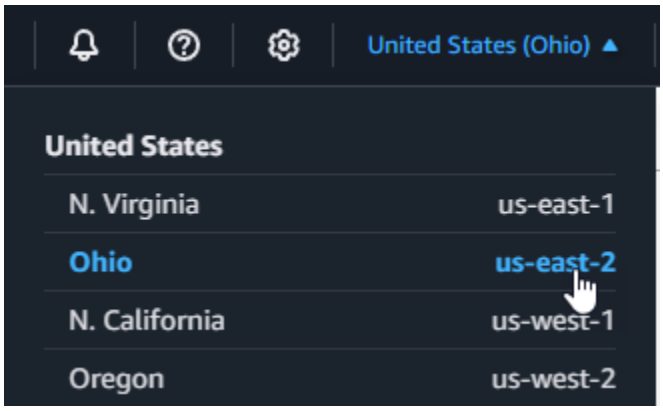
En suivant ces étapes, vous apprendrez à configurer une fonction d'événement Lambda pour qu'elle s'exécute chaque fois que des objets sont ajoutés ou supprimés d'un compartiment Amazon S3. Vous pouvez compléter ce didacticiel en n’utilisant que la Console de gestion AWS.

Créer un compartiment Amazon S3



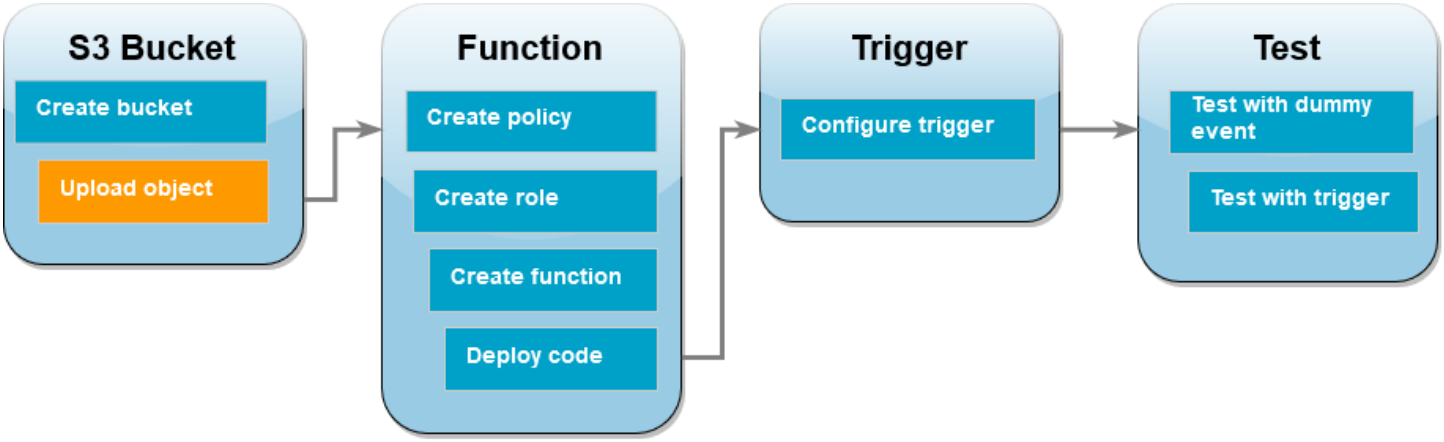
Pour créer un compartiment Amazon S3

1. Ouvrez la console Amazon S3 et sélectionnez la page Compartiments à usage général.
2. Sélectionnez le Région AWS plus proche de votre situation géographique. Vous pouvez modifier votre région à l'aide de la liste déroulante en haut de l'écran. Plus loin dans le didacticiel, vous devez créer votre fonction d'événement Lambda dans la même région.



3. Choisissez Create bucket (Créer un compartiment).
4. Sous Configuration générale, procédez comme suit :
   a. Pour le type de compartiment, veillez à sélectionner Usage général.
   b. Pour le nom du compartiment, saisissez un nom unique au monde qui respecte les règles de dénomination du compartiment Amazon S3. Les noms de compartiment peuvent contenir uniquement des lettres minuscules, des chiffres, de points (.) et des traits d'union (-).
5. Conservez les valeurs par défaut de toutes les autres options et choisissez Créer un compartiment.

Charger un objet de test dans votre compartiment

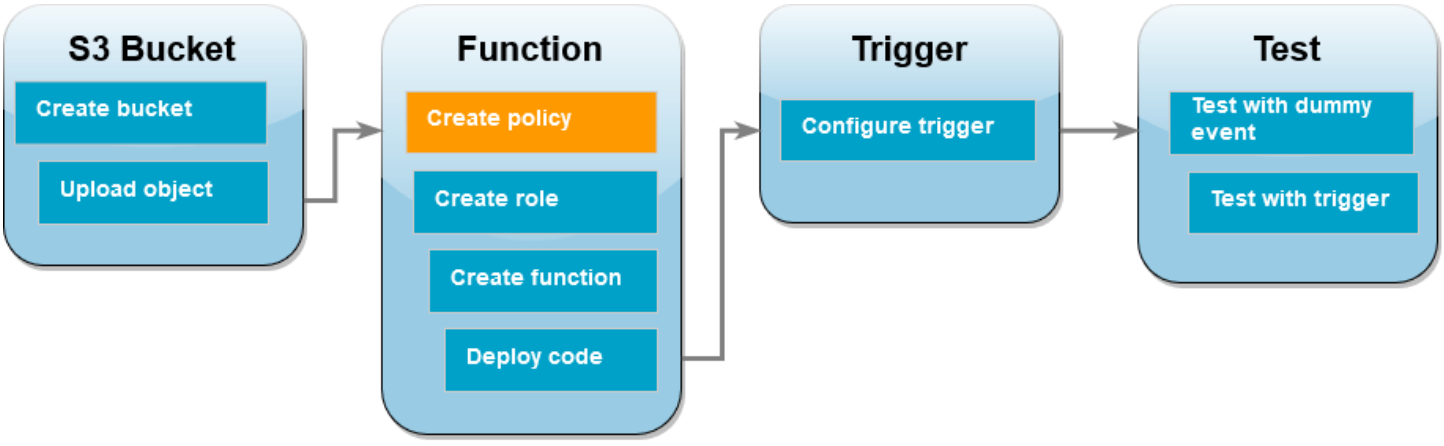


Pour charger un objet de test

1. Ouvrez la page Compartiments de la console Amazon S3 et choisissez le compartiment que vous avez créé à l'étape précédente.
2. Choisissez Charger.
3. Choisissez Ajouter des fichiers et sélectionnez l'objet que vous souhaitez charger. Vous pouvez sélectionner n'importe quel fichier (par exemple, `HappyFace.jpg`).
4. Choisissez Ouvrir, puis Charger.

Plus loin dans le didacticiel, vous testerez votre fonction d'événement Lambda à l'aide de cet objet.

Création d'une stratégie d'autorisations



Créez une politique d'autorisation qui permet à Lambda d'obtenir des objets depuis un compartiment Amazon S3 et d'écrire dans Amazon CloudWatch Logs.

Pour créer la politique

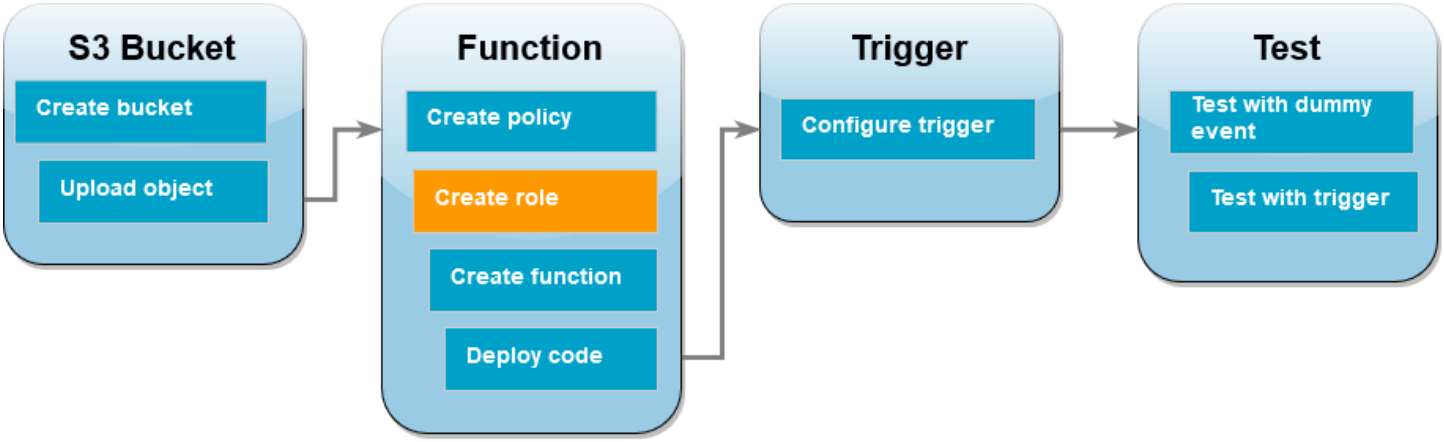
1. Ouvrez la page stratégies de la console IAM.
2. Choisissez Créer une stratégie.
3. Choisissez l'onglet JSON, puis collez la stratégie personnalisée suivante dans l'éditeur JSON.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents",
                "logs:CreateLogGroup",
                "logs:CreateLogStream"
            ],
            "Resource": "arn:aws:logs:*:*:*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": "arn:aws:s3:::*/*"
        }
    ]
}
```

4. Choisissez Suivant : Balises.
5. Choisissez Suivant : Vérification.
6. Sous Examiner une stratégie, pour le Nom de la stratégie, saisissez **`s3-trigger-tutorial`**.
7. Choisissez Créer une stratégie.

Créer un rôle d’exécution

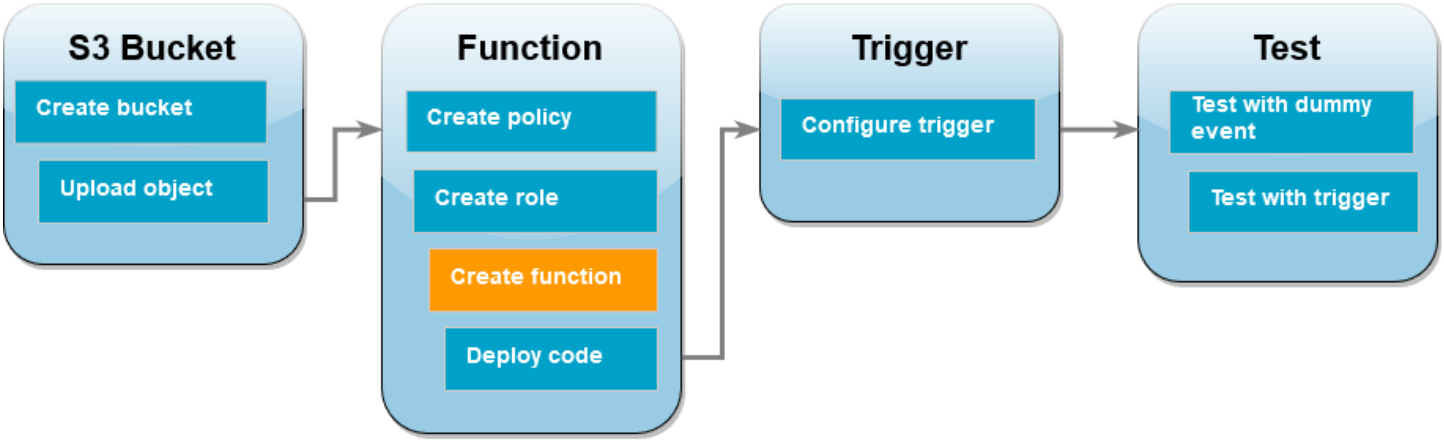


Un rôle d'exécution est un rôle Gestion des identités et des accès AWS (IAM) qui accorde à une fonction d'événement Lambda l'autorisation d' Services AWS accès et de ressources. Dans cette étape, vous créez un rôle d’exécution à l’aide de la politique d’autorisations que vous avez créée à l’étape précédente.

Pour créer un rôle d’exécution et attacher votre politique d’autorisations personnalisée

1. Ouvrez la page Rôles de la console IAM.
2. Sélectionnez Créer un rôle.
3. Pour le type d’entité de confiance, choisissez Service AWS , puis pour le cas d’utilisation, choisissez Lambda.
4. Choisissez Suivant.
5. Dans la zone de recherche de stratégie, entrez **`s3-trigger-tutorial`**.
6. Dans les résultats de la recherche, sélectionnez la stratégie que vous avez créée (`s3-trigger-tutorial`), puis choisissez Suivant.
7. Sous Role details (Détails du rôle), pour Role name (Nom du rôle), saisissez **`lambda-s3-trigger-role`**, puis sélectionnez Create role (Créer un rôle).

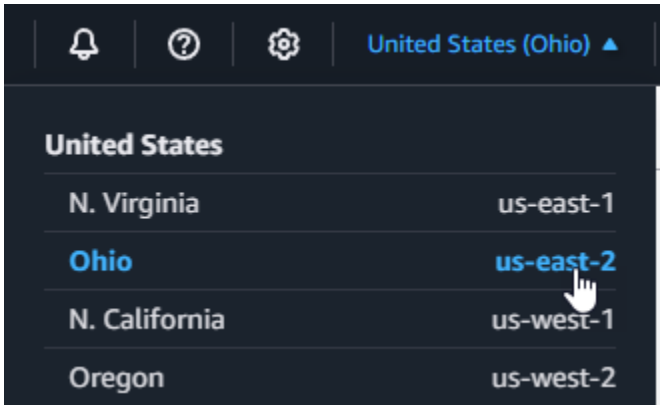
Création de la fonction d'événement Lambda



Créez une fonction d'événement Lambda dans la console à l'aide du moteur d'exécution Python 3.14.

Pour créer la fonction d'événement Lambda

1. Ouvrez la page Event Functions de la console Lambda.
2. Assurez-vous de travailler dans le même environnement que celui dans Région AWS lequel vous avez créé votre compartiment Amazon S3. Vous pouvez modifier votre région à l'aide de la liste déroulante en haut de l'écran.



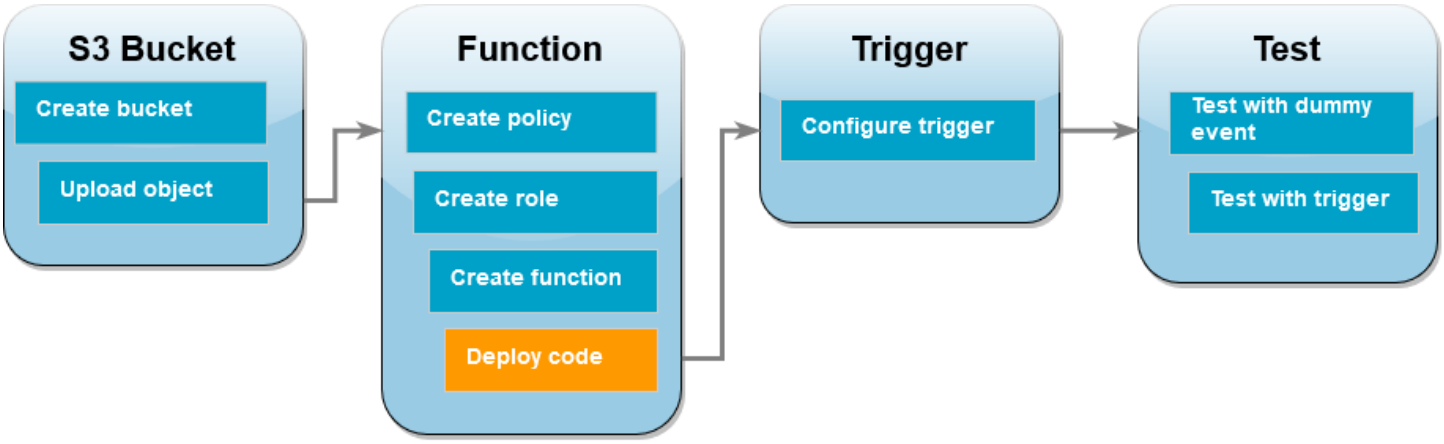
3. Choisissez Create Event Function.
4. Choisissez Créer à partir de zéro.
5. Sous Basic information (Informations de base), procédez comme suit :
   a. Sous Nom de la fonction, saisissez `s3-trigger-tutorial`.
   b. Pour Runtime, choisissez Python 3.14.
   c. Pour Architecture, choisissez x86_64.
6. Dans l'onglet Modifier le rôle d'exécution par défaut, procédez comme suit :

a. Ouvrez l'onglet, puis choisissez Utiliser un rôle existant.

b. Sélectionnez le `lambda-s3-trigger-role` que vous avez créé précédemment.

7. Choisissez Create Event Function.

Déployer le code de la fonction d'événement



Ce didacticiel utilise le moteur d'exécution Python 3.14, mais nous avons également fourni des exemples de fichiers de code pour d'autres environnements d'exécution. Vous pouvez sélectionner l'onglet dans la zone suivante pour voir le code du moteur d'exécution qui vous intéresse.

La fonction d'événement Lambda récupère le nom clé de l'objet chargé et le nom du compartiment à partir du `event` paramètre qu'il reçoit d'Amazon S3. La fonction utilise ensuite la méthode get_object du AWS SDK pour Python (Boto3) pour récupérer les métadonnées de l'objet, y compris le type de contenu (type MIME) de l'objet chargé.

Pour déployer le code de la fonction d'événement

1. Choisissez l'onglet Python dans la zone suivante et copiez le code.

   .NET

   SDK pour .NET

   > **Note**
   >
   > Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Utilisation d'un événement S3 avec Lambda en utilisant .NET.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
using System.Threading.Tasks;
using Amazon.Lambda.Core;
using Amazon.S3;
using System;
using Amazon.Lambda.S3Events;
using System.Web;

// Assembly attribute to enable the Lambda function's JSON input to be
 converted into a .NET class.
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJson

namespace S3Integration
{
    public class Function
    {
        private static AmazonS3Client _s3Client;
        public Function() : this(null)
        {
        }

        internal Function(AmazonS3Client s3Client)
        {
            _s3Client = s3Client ?? new AmazonS3Client();
        }

        public async Task<string> Handler(S3Event evt, ILambdaContext
 context)
        {
            try
            {
                if (evt.Records.Count <= 0)
                {
                    context.Logger.LogLine("Empty S3 Event received");
                    return string.Empty;
                }

                var bucket = evt.Records[0].S3.Bucket.Name;
```

```
                var key =
 HttpUtility.UrlDecode(evt.Records[0].S3.Object.Key);

                context.Logger.LogLine($"Request is for {bucket} and {key}");

                var objectResult = await _s3Client.GetObjectAsync(bucket,
 key);

                context.Logger.LogLine($"Returning {objectResult.Key}");

                return objectResult.Key;
            }
            catch (Exception e)
            {
                context.Logger.LogLine($"Error processing request -
 {e.Message}");

                return string.Empty;
            }
        }
    }
}
```

Go

Kit SDK pour Go V2

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Utilisation d'un événement S3 avec Lambda en utilisant Go.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package main

import (
 "context"
```

```
 "log"

 "github.com/aws/aws-lambda-go/events"
 "github.com/aws/aws-lambda-go/lambda"
 "github.com/aws/aws-sdk-go-v2/config"
 "github.com/aws/aws-sdk-go-v2/service/s3"
)

func handler(ctx context.Context, s3Event events.S3Event) error {
 sdkConfig, err := config.LoadDefaultConfig(ctx)
 if err != nil {
  log.Printf("failed to load default config: %s", err)
  return err
 }
 s3Client := s3.NewFromConfig(sdkConfig)

 for _, record := range s3Event.Records {
  bucket := record.S3.Bucket.Name
  key := record.S3.Object.URLDecodedKey
  headOutput, err := s3Client.HeadObject(ctx, &s3.HeadObjectInput{
   Bucket: &bucket,
   Key:    &key,
  })
  if err != nil {
   log.Printf("error getting head of object %s/%s: %s", bucket, key, err)
   return err
  }
  log.Printf("successfully retrieved %s/%s of type %s", bucket, key,
 *headOutput.ContentType)
 }

 return nil
}

func main() {
 lambda.Start(handler)
}
```

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Utilisation d'un événement S3 avec Lambda en utilisant Go.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package example;

import software.amazon.awssdk.services.s3.model.HeadObjectRequest;
import software.amazon.awssdk.services.s3.model.HeadObjectResponse;
import software.amazon.awssdk.services.s3.S3Client;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.S3Event;
import
 com.amazonaws.services.lambda.runtime.events.models.s3.S3EventNotification.S3EventNo

import org.slf4j.Logger;
import org.slf4j.LoggerFactory;

public class Handler implements RequestHandler<S3Event, String> {
    private static final Logger logger =
 LoggerFactory.getLogger(Handler.class);
    @Override
    public String handleRequest(S3Event s3event, Context context) {
        try {
          S3EventNotificationRecord record = s3event.getRecords().get(0);
          String srcBucket = record.getS3().getBucket().getName();
          String srcKey = record.getS3().getObject().getUrlDecodedKey();

          S3Client s3Client = S3Client.builder().build();
```

```
          HeadObjectResponse headObject = getHeadObject(s3Client, srcBucket,
 srcKey);

          logger.info("Successfully retrieved " + srcBucket + "/" + srcKey +
 " of type " + headObject.contentType());

          return "Ok";
        } catch (Exception e) {
          throw new RuntimeException(e);
        }
    }

    private HeadObjectResponse getHeadObject(S3Client s3Client, String
 bucket, String key) {
        HeadObjectRequest headObjectRequest = HeadObjectRequest.builder()
                .bucket(bucket)
                .key(key)
                .build();
        return s3Client.headObject(headObjectRequest);
    }
}
```

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement S3 avec Lambda en utilisant. JavaScript

```
import { S3Client, HeadObjectCommand } from "@aws-sdk/client-s3";

const client = new S3Client();

export const handler = async (event, context) => {

    // Get the object from the event and show its content type
```

```
    const bucket = event.Records[0].s3.bucket.name;
    const key = decodeURIComponent(event.Records[0].s3.object.key.replace(/\
+/g, ' '));

    try {
        const { ContentType } = await client.send(new HeadObjectCommand({
            Bucket: bucket,
            Key: key,
        }));

        console.log('CONTENT TYPE:', ContentType);
        return ContentType;

    } catch (err) {
        console.log(err);
        const message = `Error getting object ${key} from bucket ${bucket}.
 Make sure they exist and your bucket is in the same region as this
 function.`;
        console.log(message);
        throw new Error(message);
    }
};
```

Consommation d'un événement S3 avec Lambda en utilisant. TypeScript

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import { S3Event } from 'aws-lambda';
import { S3Client, HeadObjectCommand } from '@aws-sdk/client-s3';

const s3 = new S3Client({ region: process.env.AWS_REGION });

export const handler = async (event: S3Event): Promise<string | undefined> =>
 {
  // Get the object from the event and show its content type
  const bucket = event.Records[0].s3.bucket.name;
  const key = decodeURIComponent(event.Records[0].s3.object.key.replace(/\+/
g, ' '));
  const params = {
    Bucket: bucket,
    Key: key,
  };
```

```
  try {
    const { ContentType } = await s3.send(new HeadObjectCommand(params));
    console.log('CONTENT TYPE:', ContentType);
    return ContentType;
  } catch (err) {
    console.log(err);
    const message = `Error getting object ${key} from bucket ${bucket}. Make
 sure they exist and your bucket is in the same region as this function.`;
    console.log(message);
    throw new Error(message);
  }
};
```

PHP

Kit SDK pour PHP

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement S3 avec Lambda à l'aide de PHP.

```
<?php

use Bref\Context\Context;
use Bref\Event\S3\S3Event;
use Bref\Event\S3\S3Handler;
use Bref\Logger\StderrLogger;

require __DIR__ . '/vendor/autoload.php';


class Handler extends S3Handler
{
    private StderrLogger $logger;
    public function __construct(StderrLogger $logger)
    {
        $this->logger = $logger;
```

```
    }

    public function handleS3(S3Event $event, Context $context) : void
    {
        $this->logger->info("Processing S3 records");

        // Get the object from the event and show its content type
        $records = $event->getRecords();

        foreach ($records as $record)
        {
            $bucket = $record->getBucket()->getName();
            $key = urldecode($record->getObject()->getKey());

            try {
                $fileSize = urldecode($record->getObject()->getSize());
                echo "File Size: " . $fileSize . "\n";
                // TODO: Implement your custom processing logic here
            } catch (Exception $e) {
                echo $e->getMessage() . "\n";
                echo 'Error getting object ' . $key . ' from bucket ' .
 $bucket . '. Make sure they exist and your bucket is in the same region as
 this function.' . "\n";
                throw $e;
            }
        }
    }
}

$logger = new StderrLogger();
return new Handler($logger);
```

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Utilisation d'un événement S3 avec Lambda en utilisant Python.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
import json
import urllib.parse
import boto3

print('Loading function')

s3 = boto3.client('s3')


def lambda_handler(event, context):
    #print("Received event: " + json.dumps(event, indent=2))

    # Get the object from the event and show its content type
    bucket = event['Records'][0]['s3']['bucket']['name']
    key = urllib.parse.unquote_plus(event['Records'][0]['s3']['object']
['key'], encoding='utf-8')
    try:
        response = s3.get_object(Bucket=bucket, Key=key)
        print("CONTENT TYPE: " + response['ContentType'])
        return response['ContentType']
    except Exception as e:
        print(e)
        print('Error getting object {} from bucket {}. Make sure they
 exist and your bucket is in the same region as this function.'.format(key,
 bucket))
        raise e
```

Ruby

Kit SDK pour Ruby

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement S3 avec Lambda à l'aide de Ruby.

```
require 'json'
require 'uri'
require 'aws-sdk'

puts 'Loading function'

def lambda_handler(event:, context:)
  s3 = Aws::S3::Client.new(region: 'region') # Your AWS region
  # puts "Received event: #{JSON.dump(event)}"

  # Get the object from the event and show its content type
  bucket = event['Records'][0]['s3']['bucket']['name']
  key = URI.decode_www_form_component(event['Records'][0]['s3']['object']
['key'], Encoding::UTF_8)
  begin
    response = s3.get_object(bucket: bucket, key: key)
    puts "CONTENT TYPE: #{response.content_type}"
    return response.content_type
  rescue StandardError => e
    puts e.message
    puts "Error getting object #{key} from bucket #{bucket}. Make sure they
 exist and your bucket is in the same region as this function."
    raise e
  end
end
```

Rust

SDK pour Rust

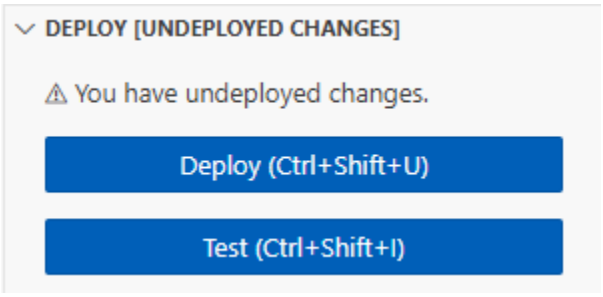
> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Utilisation d'un événement S3 avec Lambda en utilisant Rust.

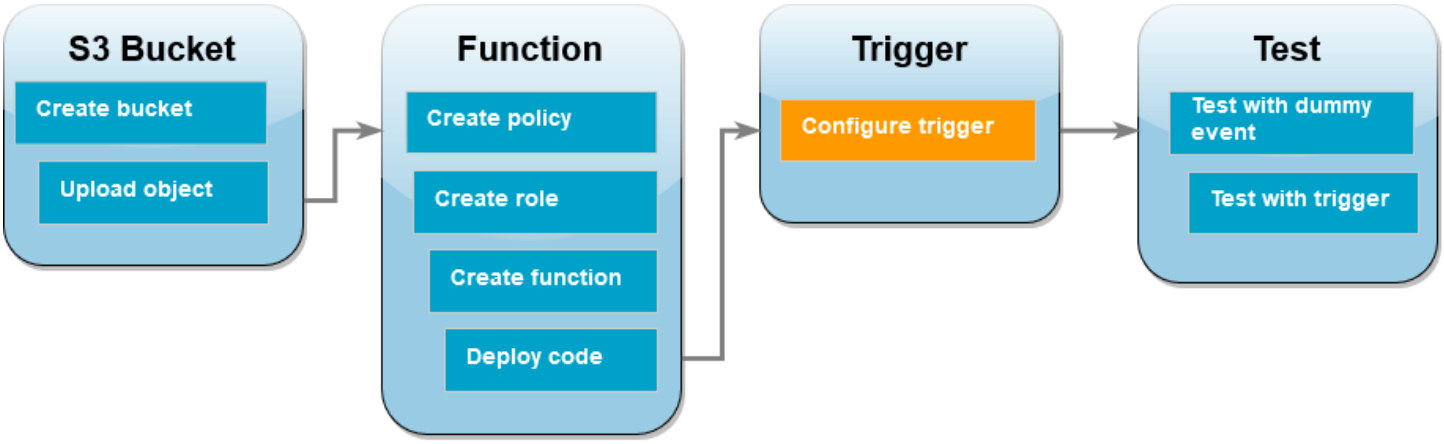
```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
use aws_lambda_events::event::s3::S3Event;
use aws_sdk_s3::{Client};
use lambda_runtime::{run, service_fn, Error, LambdaEvent};


/// Main function
#[tokio::main]
async fn main() -> Result<(), Error> {
    tracing_subscriber::fmt()
        .with_max_level(tracing::Level::INFO)
        .with_target(false)
        .without_time()
        .init();

    // Initialize the AWS SDK for Rust
    let config = aws_config::load_from_env().await;
    let s3_client = Client::new(&config);

    let res = run(service_fn(|request: LambdaEvent<S3Event>| {
        function_handler(&s3_client, request)
    })).await;

    res
}

async fn function_handler(
    s3_client: &Client,
```

```
    evt: LambdaEvent<S3Event>
) -> Result<(), Error> {
    tracing::info!(records = ?evt.payload.records.len(), "Received request
 from SQS");

    if evt.payload.records.len() == 0 {
        tracing::info!("Empty S3 event received");
    }

    let bucket =
 evt.payload.records[0].s3.bucket.name.as_ref().expect("Bucket name to
 exist");
    let key = evt.payload.records[0].s3.object.key.as_ref().expect("Object
 key to exist");

    tracing::info!("Request is for {} and object {}", bucket, key);

    let s3_get_object_result = s3_client
        .get_object()
        .bucket(bucket)
        .key(key)
        .send()
        .await;

    match s3_get_object_result {
        Ok(_) => tracing::info!("S3 Get Object success, the s3GetObjectResult
 contains a 'body' property of type ByteStream"),
        Err(_) => tracing::info!("Failure with S3 Get Object request")
    }

    Ok(())
}
```

2. Dans le volet Code source de la console Lambda, collez le code dans l'éditeur de code, en remplaçant le code créé par Lambda.
3. Dans la section DÉPLOYER, choisissez Déployer pour mettre à jour le code de votre fonction :

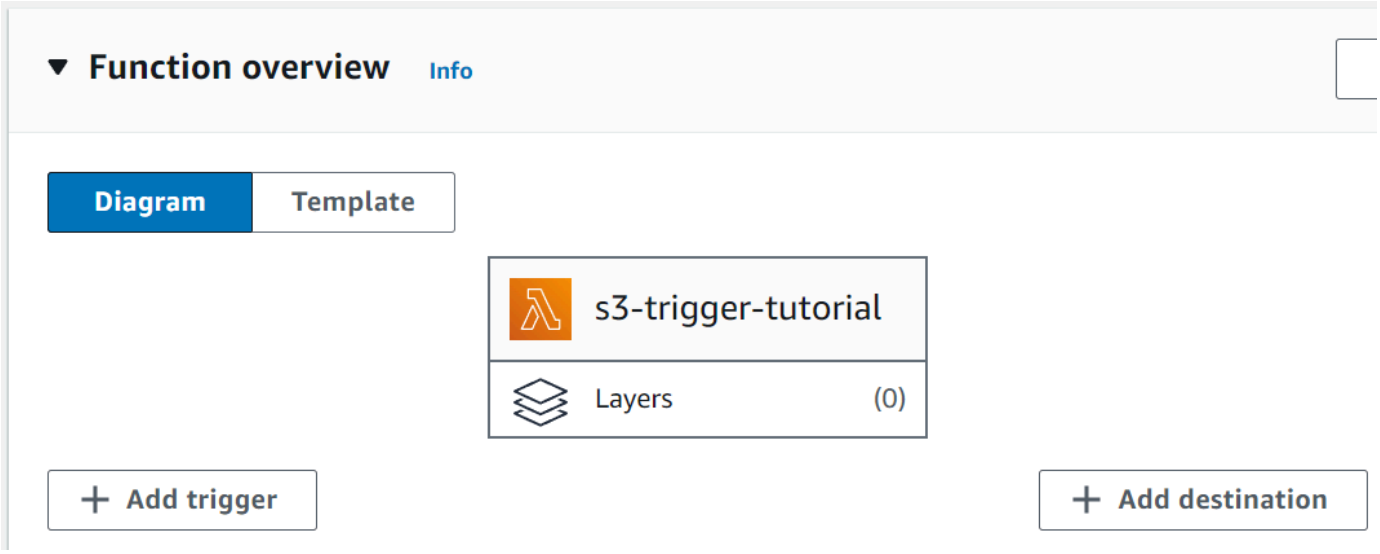


Création d'un déclencheur Amazon S3



Pour créer le déclencheur Amazon S3

1. Dans le volet de Présentation de la fonction, choisissez Ajouter un déclencheur.

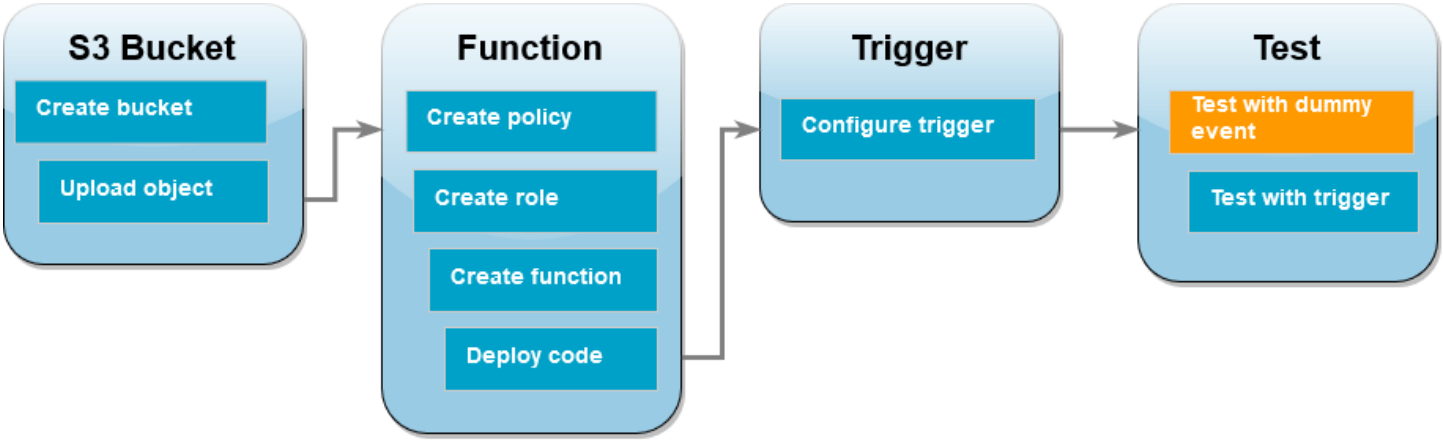


2. Sélectionnez S3.

3. Sous Compartiment, sélectionnez le compartiment que vous avez créé précédemment dans le didacticiel.
4. Sous Types d'événements, assurez-vous que Tous les événements de création d'objet est sélectionné.
5. Sous Invocation récursive, cochez la case pour confirmer qu'il n'est pas recommandé d'utiliser le même compartiment Amazon S3 pour les entrées et les sorties.
6. Choisissez Ajouter.

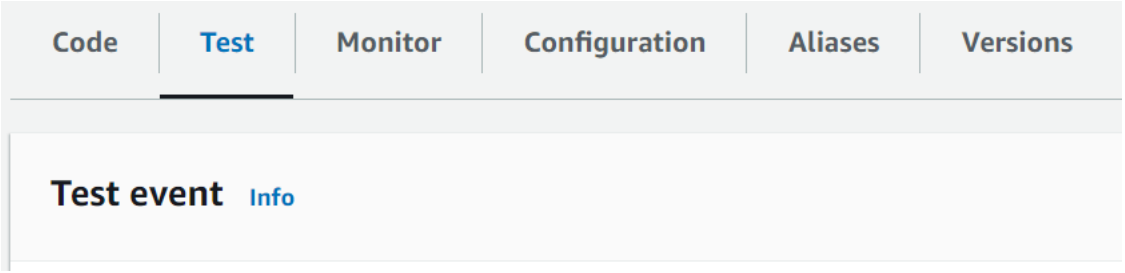
> **Note**
>
> Lorsque vous créez un déclencheur Amazon S3 pour une fonction d'événement Lambda à l'aide de la console Lambda, Amazon S3 configure une notification d'événement sur le compartiment que vous spécifiez. Avant de configurer cette notification d'événement, Amazon S3 effectue une série de vérifications pour confirmer que la destination de l'événement existe et dispose des politiques IAM requises. Amazon S3 effectue également ces tests sur toutes les autres notifications d'événements configurées pour ce compartiment.
> En raison de cette vérification, si le compartiment a déjà configuré des destinations d'événements pour des ressources qui n'existent plus ou pour des ressources qui ne disposent pas des politiques d'autorisations requises, Amazon S3 ne sera pas en mesure de créer la nouvelle notification d'événement. Vous verrez le message d'erreur suivant indiquant que votre déclencheur n'a pas pu être créé :
>
> ```
> An error occurred when creating the trigger: Unable to validate the following
>  destination configurations.
> ```
>
> Vous pouvez voir cette erreur si vous avez précédemment configuré un déclencheur pour une autre fonction d'événement Lambda utilisant le même compartiment, et si vous avez depuis supprimé la fonction ou modifié ses politiques d'autorisation.

Testez votre fonction d'événement Lambda avec un événement factice



Pour tester la fonction d'événement Lambda avec un événement factice

1. Dans la page de votre fonction de la console Lambda, choisissez l'onglet Tester.



2. Dans Event name (Nom de l'événement), saisissez `MyTestEvent`.
3. Dans le JSON d'événement, collez l'événement de test suivant. Veillez à remplacer les valeurs suivantes :

   - Remplacez `us-east-1` par la région dans laquelle vous avez créé votre compartiment Amazon S3.
   - Remplacez les deux instances de `amzn-s3-demo-bucket` par le nom de votre propre compartiment Amazon S3.
   - Remplacez `test%2FKey` par le nom de l'objet de test que vous avez chargé précédemment dans votre compartiment (par exemple, `HappyFace.jpg`).

```
{
  "Records": [
    {
      "eventVersion": "2.0",
      "eventSource": "aws:s3",
```

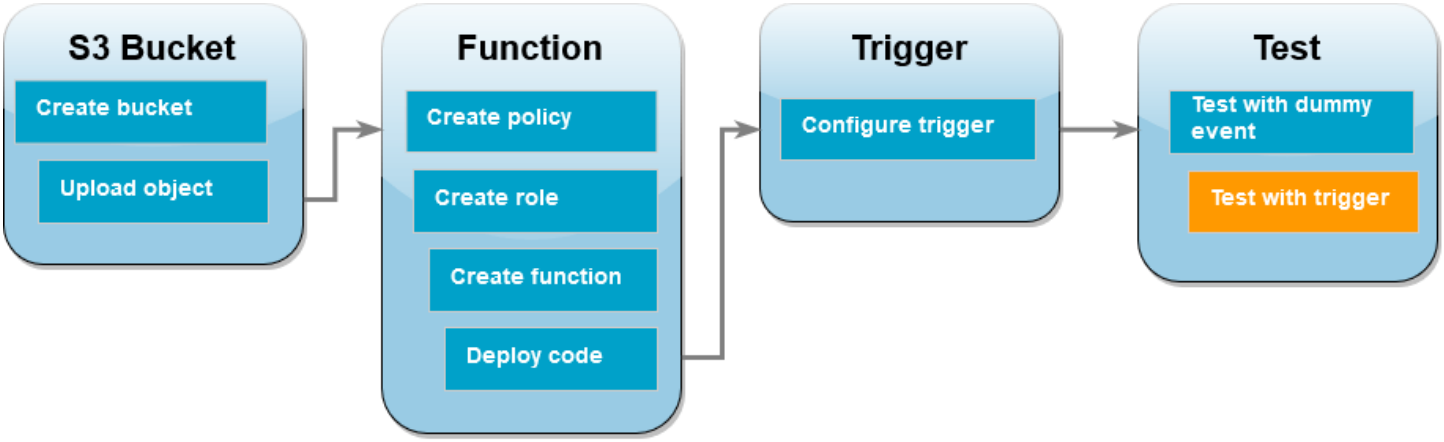
```
      "awsRegion": "us-east-1",
      "eventTime": "1970-01-01T00:00:00.000Z",
      "eventName": "ObjectCreated:Put",
      "userIdentity": {
        "principalId": "EXAMPLE"
      },
      "requestParameters": {
        "sourceIPAddress": "127.0.0.1"
      },
      "responseElements": {
        "x-amz-request-id": "EXAMPLE123456789",
        "x-amz-id-2": "EXAMPLE123/5678abcdefghijklambdaisawesome/
mnopqrstuvwxyzABCDEFGH"
      },
      "s3": {
        "s3SchemaVersion": "1.0",
        "configurationId": "testConfigRule",
        "bucket": {
          "name": "amzn-s3-demo-bucket",
          "ownerIdentity": {
            "principalId": "EXAMPLE"
          },
          "arn": "arn:aws:s3:::amzn-s3-demo-bucket"
        },
        "object": {
          "key": "test%2Fkey",
          "size": 1024,
          "eTag": "0123456789abcdef0123456789abcdef",
          "sequencer": "0A1B2C3D4E5F678901"
        }
      }
    }
  ]
}
```

4. Cliquez sur Enregistrer.
5. Sélectionnez Tester).
6. Si votre fonction s'exécute correctement, vous verrez un résultat similaire à ce qui suit dans l'onglet Résultats de l'exécution.

```
Response
"image/jpeg"
```

```
Function Logs
START RequestId: 12b3cae7-5f4e-415e-93e6-416b8f8b66e6 Version: $LATEST
2021-02-18T21:40:59.280Z    12b3cae7-5f4e-415e-93e6-416b8f8b66e6    INFO    INPUT
 BUCKET AND KEY:  { Bucket: 'amzn-s3-demo-bucket', Key: 'HappyFace.jpg' }
2021-02-18T21:41:00.215Z    12b3cae7-5f4e-415e-93e6-416b8f8b66e6    INFO    CONTENT
 TYPE: image/jpeg
END RequestId: 12b3cae7-5f4e-415e-93e6-416b8f8b66e6
REPORT RequestId: 12b3cae7-5f4e-415e-93e6-416b8f8b66e6    Duration: 976.25 ms
 Billed Duration: 977 ms    Memory Size: 128 MB    Max Memory Used: 90 MB    Init
 Duration: 430.47 ms

Request ID
12b3cae7-5f4e-415e-93e6-416b8f8b66e6
```

Testez la fonction d'événement Lambda avec le déclencheur Amazon S3



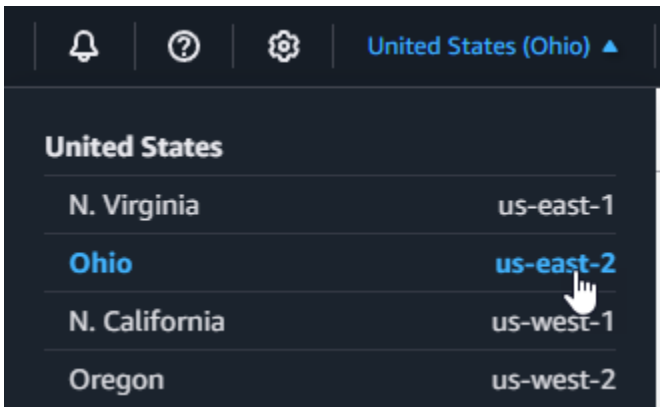
Pour tester votre fonction avec le déclencheur configuré, chargez un objet dans votre compartiment Amazon S3 à l'aide de la console. Pour vérifier que votre fonction d'événement Lambda s'est exécutée comme prévu, utilisez CloudWatch Logs pour afficher le résultat de votre fonction.

Pour charger un objet dans votre compartiment Amazon S3

1. Ouvrez la page Compartiments de la console Amazon S3 et choisissez le compartiment que vous avez créé précédemment.
2. Choisissez Charger.
3. Choisissez Ajouter des fichiers et utilisez le sélecteur de fichiers pour choisir l'objet que vous souhaitez charger. Cet objet peut être n'importe quel fichier que vous choisissez.
4. Choisissez Ouvrir, puis Charger.

Pour vérifier l'invocation de la fonction d'événement à l'aide des journaux CloudWatch

1. Ouvrez la console CloudWatch.
2. Assurez-vous de travailler de la même manière que celle dans laquelle Région AWS vous avez créé votre fonction d'événement Lambda. Vous pouvez modifier votre région à l'aide de la liste déroulante en haut de l'écran.



3. Choisissez Journaux, puis Groupes de journaux.
4. Choisissez le groupe de journaux de votre fonction (`/aws/lambda/s3-trigger-tutorial`).
5. Sous Flux de journaux, sélectionnez le flux de journaux le plus récent.
6. Si votre fonction a été invoquée correctement en réponse à votre déclencheur Amazon S3, vous verrez un résultat similaire à ce qui suit. Le `CONTENT TYPE` que vous voyez dépend du type de fichier que vous avez chargé dans votre compartiment.

```
2022-05-09T23:17:28.702Z 0cae7f5a-b0af-4c73-8563-a3430333cc10 INFO CONTENT
 TYPE: image/jpeg
```

Nettoyage de vos ressources

Vous pouvez maintenant supprimer les ressources que vous avez créées pour ce didacticiel, sauf si vous souhaitez les conserver. En supprimant AWS les ressources que vous n'utilisez plus, vous évitez des frais inutiles pour votre Compte AWS.

Pour supprimer la fonction d'événement Lambda

1. Ouvrez la page Event Functions de la console Lambda.
2. Sélectionnez la fonction d'événement que vous avez créée.
3. Sélectionnez Actions, Supprimer.

4. Saisissez **`confirm`** dans la zone de saisie de texte et choisissez Delete (Supprimer).

Pour supprimer le rôle d'exécution

1. Ouvrez la page Roles (Rôles) de la console IAM.
2. Sélectionnez le rôle d'exécution que vous avez créé.
3. Sélectionnez Supprimer.
4. Saisissez le nom du rôle dans le champ de saisie de texte et choisissez Delete (Supprimer).

Pour supprimer le compartiment S3

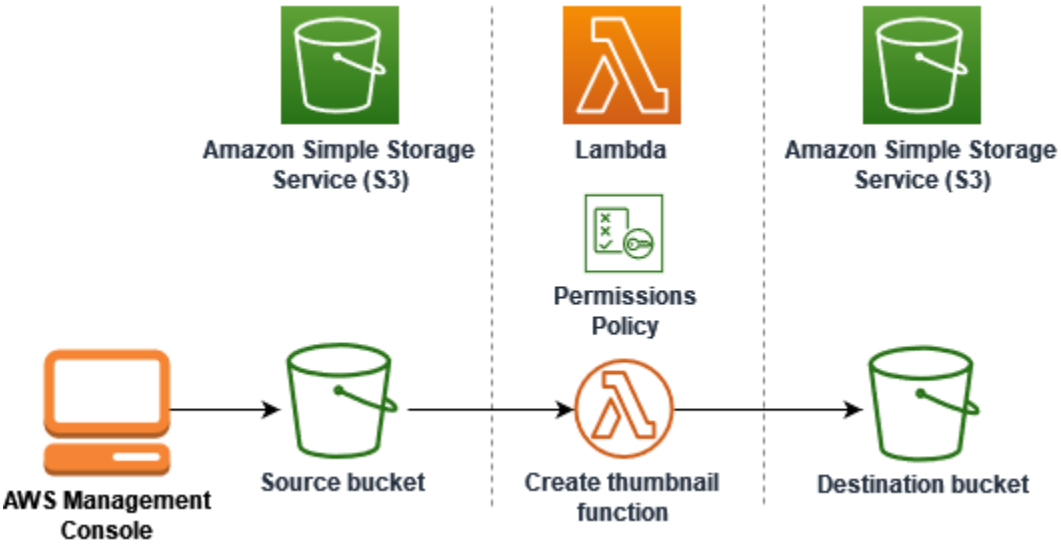
1. Ouvrez la console Amazon S3.
2. Sélectionnez le compartiment que vous avez créé.
3. Sélectionnez Supprimer.
4. Saisissez le nom du compartiment dans le champ de saisie de texte.
5. Choisissez Supprimer le compartiment.

Étapes suivantes

Dans Didacticiel : Utilisation d'un déclencheur Amazon S3 pour créer des images miniatures, le déclencheur Amazon S3 invoque une fonction qui crée une image de miniature pour chaque fichier image qui est chargé dans votre compartiment. Ce didacticiel nécessite un niveau modéré de connaissance du AWS domaine Lambda. Il montre comment créer des ressources à l'aide de AWS Command Line Interface (AWS CLI) et comment créer un package de déploiement d'archives de fichiers .zip pour la fonction et ses dépendances.

Didacticiel : Utilisation d'un déclencheur Amazon S3 pour créer des images miniatures

Dans ce didacticiel, vous allez créer et configurer une fonction d'événement Lambda qui redimensionne les images ajoutées à un bucket Amazon Simple Storage Service (Amazon S3). Lorsque vous ajoutez un fichier image à votre compartiment, Amazon S3 invoque votre fonction d'événement Lambda. La fonction crée ensuite une version miniature de l'image et l'envoie vers un autre compartiment Amazon S3.



Pour compléter ce didacticiel, effectuez les tâches suivantes :

1. Créez des compartiments Amazon S3 source et de destination et chargez un exemple d'image.
2. Créez une fonction d'événement Lambda qui redimensionne une image et génère une miniature dans un compartiment Amazon S3.
3. Configurez un déclencheur Lambda qui invoque votre fonction lorsque des objets sont chargés dans votre compartiment source.
4. Testez votre fonction, d'abord avec un événement fictif, puis en chargeant une image dans votre compartiment source.

En suivant ces étapes, vous apprendrez à utiliser Lambda pour effectuer une tâche de traitement de fichiers sur des objets ajoutés à un compartiment Amazon S3. Vous pouvez suivre ce didacticiel en utilisant le AWS Command Line Interface (AWS CLI) ou le Console de gestion AWS.

Si vous recherchez un exemple plus simple pour apprendre à configurer un déclencheur Amazon S3 pour Lambda, vous pouvez consulter le Didacticiel : utilisation d'un déclencheur Amazon S3 pour invoquer une fonction Lambda.

Rubriques

- Conditions préalables
- Création de deux compartiments Amazon S3
- Charger une image de test dans votre compartiment source
- Création d'une stratégie d'autorisations

- Créer un rôle d’exécution
- Création du package de déploiement de la fonction d'événement
- Création de la fonction d'événement Lambda
- Configurer Amazon S3 pour appeler la fonction d'événement
- Testez votre fonction d'événement Lambda avec un événement factice
- Testez votre fonction d'événement à l'aide du déclencheur Amazon S3
- Nettoyage de vos ressources

Conditions préalables

Si vous souhaitez utiliser le AWS CLI pour terminer le didacticiel, installez la dernière version du AWS Command Line Interface.

Pour le code de votre fonction d'événement Lambda, vous pouvez utiliser Python ou. Node.js Installez les outils de prise en charge linguistique et un gestionnaire de packages pour le langage que vous souhaitez utiliser.

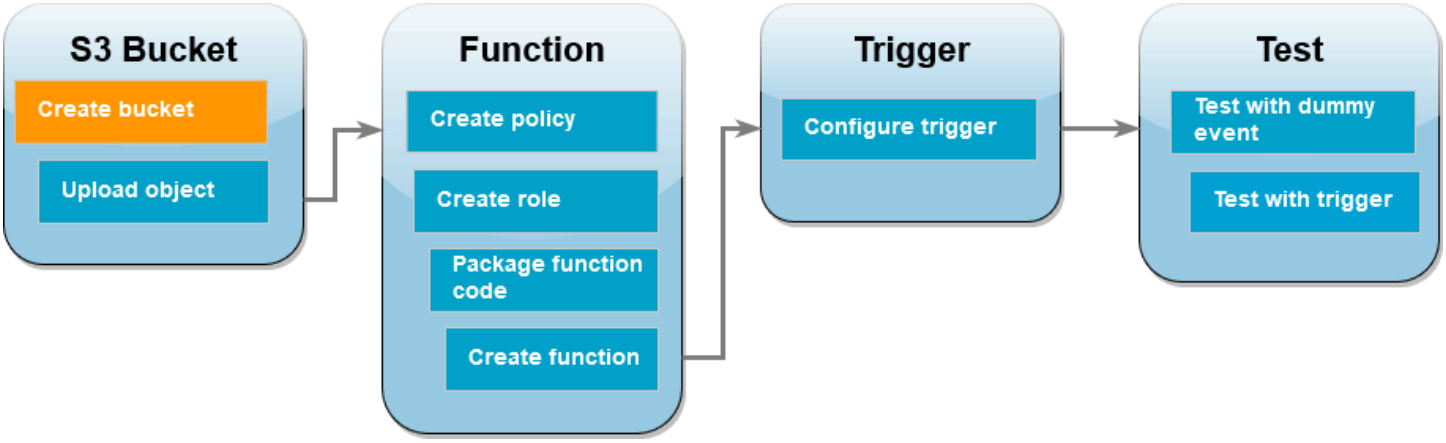
Installer la AWS Command Line Interface

Si vous ne l'avez pas encore installé AWS Command Line Interface, suivez les étapes décrites dans la section Installation ou mise à jour de la dernière version du AWS CLI pour l'installer.

Ce tutoriel nécessite un terminal de ligne de commande ou un shell pour exécuter les commandes. Sous Linux et macOS, utilisez votre gestionnaire de shell et de package préféré.

> **Note**
>
> Sous Windows, certaines commandes CLI Bash que vous utilisez couramment avec Lambda (par exemple `zip`) ne sont pas prises en charge par les terminaux intégrés du système d’exploitation. Pour obtenir une Windows-integrated version d'Ubuntu et de Bash, installez le sous-système Windows pour Linux.

Création de deux compartiments Amazon S3

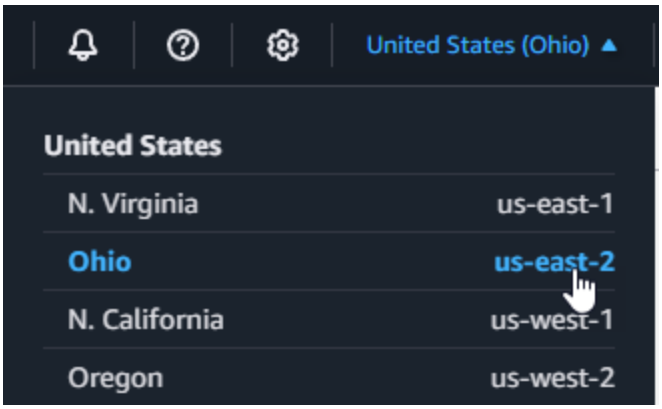


Créez d'abord deux compartiments Amazon S3. Le premier compartiment est le compartiment source dans lequel vous chargez vos images. Le second compartiment est utilisé par Lambda pour enregistrer la miniature redimensionnée lorsque vous invoquez votre fonction.

Console de gestion AWS

Pour créer les compartiments Amazon S3 (console)

1. Ouvrez la console Amazon S3 et sélectionnez la page Compartiments à usage général.
2. Sélectionnez le Région AWS plus proche de votre situation géographique. Vous pouvez modifier votre région à l'aide de la liste déroulante en haut de l'écran. Plus loin dans le didacticiel, vous devez créer votre fonction d'événement Lambda dans la même région.



3. Choisissez Create bucket (Créer un compartiment).
4. Sous Configuration générale, procédez comme suit :

   a. Pour le type de compartiment, veillez à sélectionner Usage général.

b. Pour le nom du compartiment, saisissez un nom unique au monde qui respecte les règles de dénomination du compartiment Amazon S3. Les noms de compartiment peuvent contenir uniquement des lettres minuscules, des chiffres, de points (.) et des traits d'union (-).

5. Conservez les valeurs par défaut de toutes les autres options et choisissez Créer un compartiment.

6. Répétez les étapes 1 à 5 pour créer votre compartiment de destination. Pour Nom du compartiment, saisissez **`amzn-s3-demo-source-bucket-resized`**, où **`amzn-s3-demo-source-bucket`** est le nom du compartiment source que vous venez de créer.

AWS CLI

Pour créer les compartiments Amazon S3 (AWS CLI)

1. Exécutez la commande CLI suivante pour créer votre compartiment source. Le nom que vous choisissez pour votre compartiment doit être unique au monde et respecter les Règles de dénomination du compartiment Amazon S3. Les noms peuvent contenir uniquement des lettres minuscules, des chiffres, de points (.) et des traits d'union (-). Pour `region` et `LocationConstraint`, choisissez la Région AWS la plus proche de votre emplacement géographique.

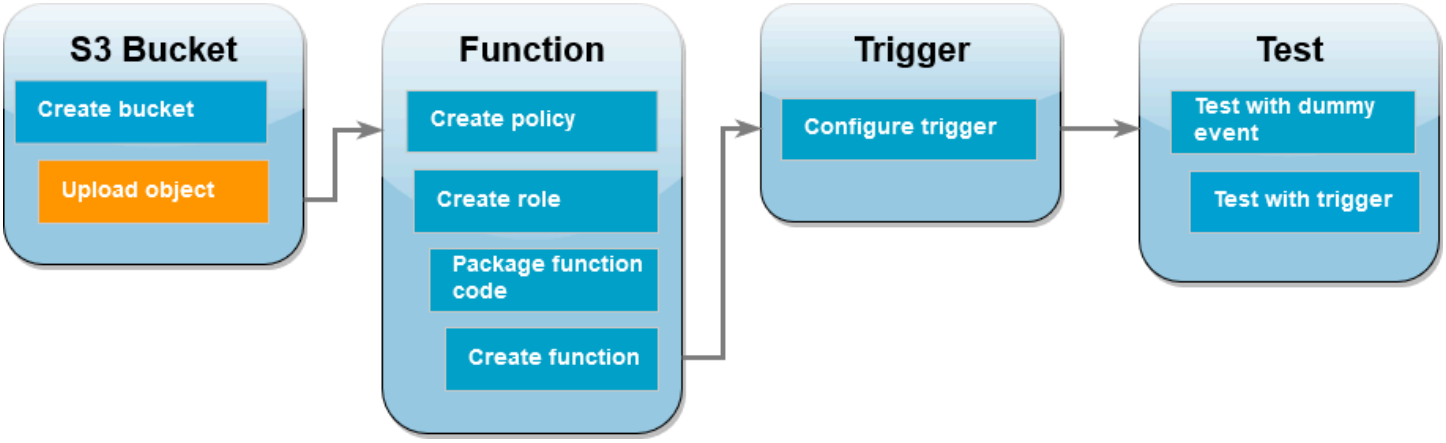
```
aws s3api create-bucket --bucket amzn-s3-demo-source-bucket --region us-east-1 \
--create-bucket-configuration LocationConstraint=us-east-1
```

Plus loin dans le didacticiel, vous devez créer votre fonction d'événement Lambda au même Région AWS endroit que votre compartiment source. Notez donc la région que vous avez choisie.

2. Exécutez la commande suivante pour créer votre compartiment de destination. Pour le nom du compartiment, vous devez utiliser **`amzn-s3-demo-source-bucket-resized`**, où **`amzn-s3-demo-source-bucket`** est le nom du compartiment source que vous avez créé à l'étape 1. Pour `region` et`LocationConstraint`, choisissez le même Région AWS que celui que vous avez utilisé pour créer votre bucket source.

```
aws s3api create-bucket --bucket amzn-s3-demo-source-bucket-resized --region us-
east-1 \
--create-bucket-configuration LocationConstraint=us-east-1
```

Charger une image de test dans votre compartiment source



Plus loin dans le didacticiel, vous testerez votre fonction d'événement Lambda en l'invoquant à l'aide de la console Lambda ou de AWS CLI la console Lambda. Pour confirmer que votre fonction fonctionne correctement, votre compartiment source doit contenir une image de test. Cette image peut être n'importe quel fichier JPG ou PNG de votre choix.

Console de gestion AWS

Pour charger une image de test dans votre compartiment source (console)

1. Ouvrez la page Compartiments de la console Amazon S3.
2. Sélectionnez le compartiment source que vous avez créé à l'étape précédente.
3. Choisissez Charger.
4. Choisissez Ajouter des fichiers et utilisez le sélecteur de fichiers pour sélectionner l'objet que vous souhaitez charger.
5. Choisissez Ouvrir, puis Charger.

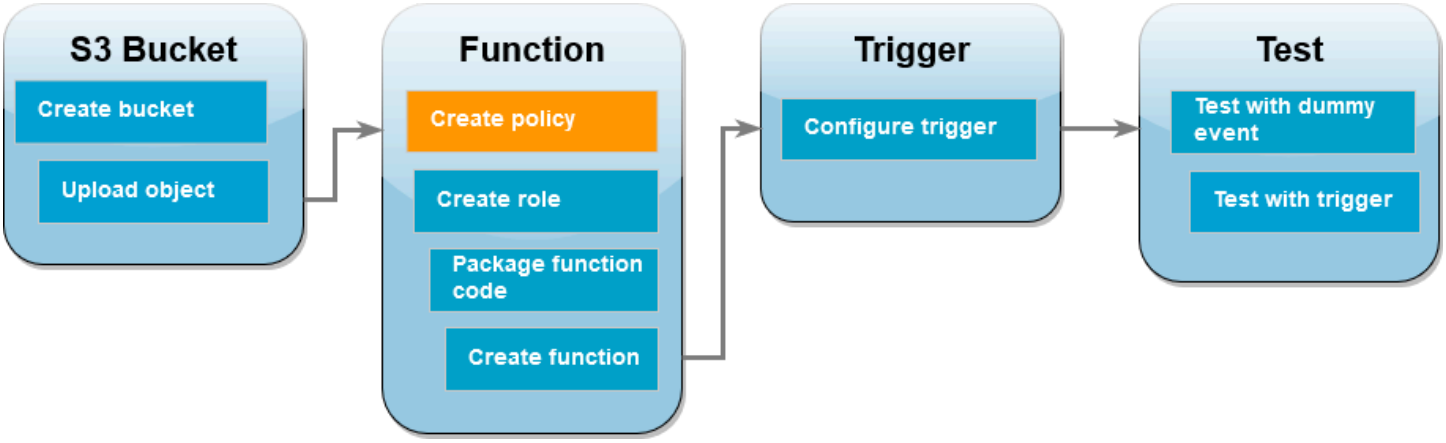
AWS CLI

Pour télécharger une image de test dans votre compartiment source (AWS CLI)

- À partir du répertoire contenant l'image que vous souhaitez charger, exécutez la commande CLI suivante. Remplacez le paramètre `--bucket` par le nom de votre compartiment source. Pour les paramètres `--key` et `--body`, utilisez le nom de fichier de votre image de test.

```
aws s3api put-object --bucket amzn-s3-demo-source-bucket --key HappyFace.jpg --
body ./HappyFace.jpg
```

Création d'une stratégie d'autorisations



La première étape de la création de votre fonction d'événement Lambda consiste à créer une politique d'autorisations. Cette politique donne à votre fonction les autorisations dont elle a besoin pour accéder à d'autres AWS ressources. Pour ce didacticiel, la politique donne à Lambda des autorisations de lecture et d'écriture pour les compartiments Amazon S3 et lui permet d'écrire dans Amazon Logs. CloudWatch

Console de gestion AWS

Pour créer une politique (console)

1. Ouvrez la page Politiques de la console Gestion des identités et des accès AWS (IAM).
2. Choisissez Create Policy (Créer une politique).
3. Choisissez l'onglet JSON, puis collez la stratégie personnalisée suivante dans l'éditeur JSON.

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents",
                "logs:CreateLogGroup",
                "logs:CreateLogStream"
            ],
            "Resource": "arn:aws:logs:*:*:*"
        },
```

```
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": "arn:aws:s3:::*/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::*/*"
        }
    ]
}
```

4. Choisissez Suivant.
5. Sous Détails de la politique, pour le Nom de la politique, saisissez **`LambdaS3Policy`**.
6. Choisissez Create Policy (Créer une politique).

AWS CLI

Pour créer la politique (AWS CLI)

1. Enregistrez le JSON suivant dans un fichier nommé `policy.json`.

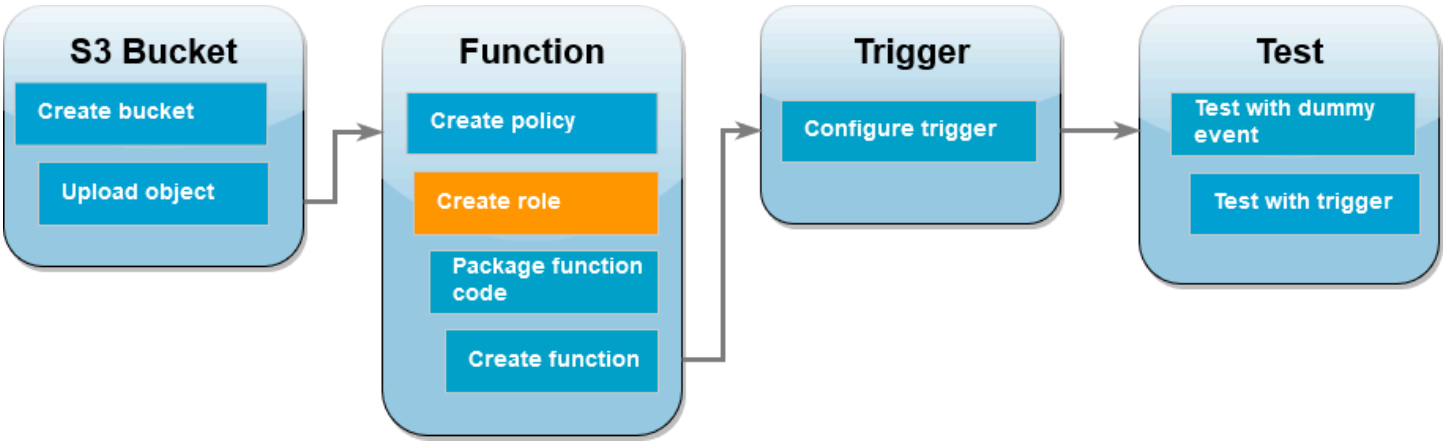
```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents",
                "logs:CreateLogGroup",
                "logs:CreateLogStream"
            ],
            "Resource": "arn:aws:logs:*:*:*"
        },
        {
            "Effect": "Allow",
```

```
            "Action": [
                "s3:GetObject"
            ],
            "Resource": "arn:aws:s3:::*/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::*/*"
        }
    ]
}
```

2. À partir du répertoire dans lequel vous avez enregistré le document de politique JSON, exécutez la commande CLI suivante.

```
aws iam create-policy --policy-name LambdaS3Policy --policy-document file://
policy.json
```

Créer un rôle d’exécution



Un rôle d'exécution est un rôle IAM qui accorde à une fonction d'événement Lambda l'autorisation d' Services AWS accès et de ressources. Pour donner à votre fonction un accès en lecture et en écriture à un compartiment Amazon S3, vous attachez la politique d’autorisation que vous avez créée à l’étape précédente.

Console de gestion AWS

Pour créer un rôle d'exécution et attacher votre politique d'autorisations (console)

1. Accédez à la Page Rôles de la console (IAM).
2. Choisissez Créer un rôle.
3. Pour Type d'entité fiable, sélectionnez Service AWS, et pour Cas d'utilisation, sélectionnez Lambda.
4. Choisissez Suivant.
5. Ajoutez la politique d'autorisations que vous avez créée à l'étape précédente en procédant comme suit :
   a. Dans la zone de recherche de stratégie, entrez **`LambdaS3Policy`**.
   b. Dans les résultats de la recherche, cochez la case pour `LambdaS3Policy`.
   c. Choisissez Suivant.
6. Sous Détails du rôle, pour le Nom du rôle entrez **`LambdaS3Role`**.
7. Choisissez Créer un rôle.

AWS CLI

Pour créer un rôle d'exécution et y associer votre politique d'autorisations (AWS CLI)

1. Enregistrez le JSON suivant dans un fichier nommé `trust-policy.json`. Cette politique de confiance permet à Lambda d'utiliser les autorisations du rôle en autorisant le principal `lambda.amazonaws.com` du service à appeler l'action AWS Security Token Service (AWS STS)`AssumeRole`.

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
```

```
  ]
}
```

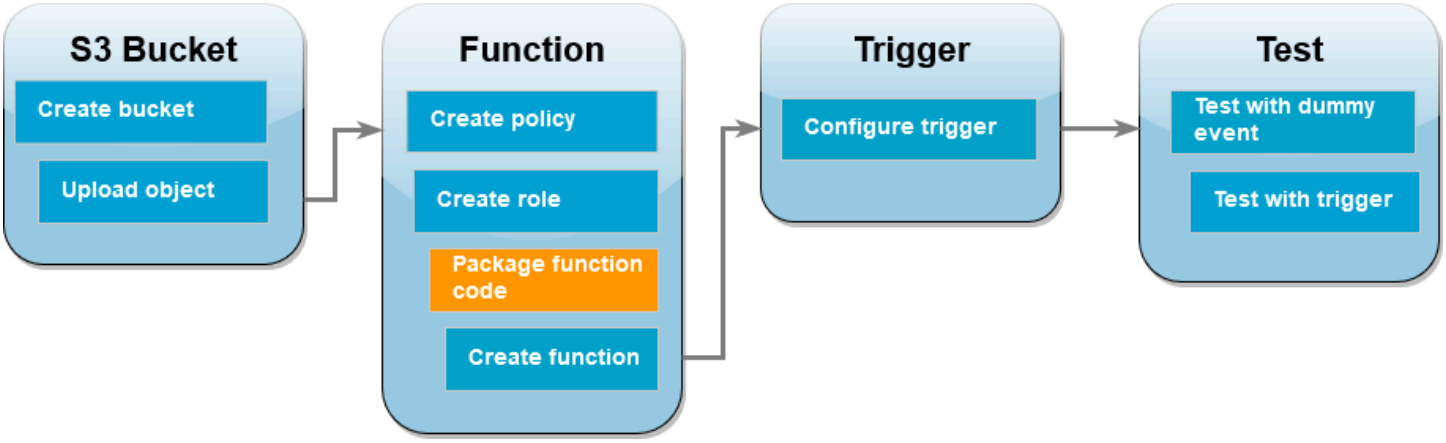
2. À partir du répertoire dans lequel vous avez enregistré le document de politique d'approbation JSON, exécutez la commande CLI suivante pour créer le rôle d'exécution.

```
aws iam create-role --role-name LambdaS3Role --assume-role-policy-document
 file://trust-policy.json
```

3. Pour attacher la politique d'autorisations que vous avez créée à l'étape précédente, exécutez la commande CLI suivante. Remplacez le Compte AWS numéro indiqué dans l'ARN de la politique par votre propre numéro de compte.

```
aws iam attach-role-policy --role-name LambdaS3Role --policy-arn
 arn:aws:iam::123456789012:policy/LambdaS3Policy
```

Création du package de déploiement de la fonction d'événement



Pour créer votre fonction, vous créez un package de déploiement contenant le code de votre fonction et ses dépendances. Pour cette fonction `CreateThumbnail`, votre code de fonction utilise une bibliothèque distincte pour le redimensionnement de l'image. Suivez les instructions correspondant à la langue de votre choix pour créer un package de déploiement contenant la bibliothèque requise.

Node.js

Pour créer le package de déploiement (Node.js)

1. Créez un répertoire nommé `lambda-s3` pour votre code de fonction et vos dépendances et accédez-y.

```
mkdir lambda-s3
cd lambda-s3
```

2. Créez un nouveau Node.js projet avecnpm. Appuyez sur `Enter` pour accepter les options par défaut fournies dans l'expérience interactive.

```
npm init
```

3. Enregistrez le code de fonction suivant dans un fichier nommé `index.mjs`. Assurez-vous de remplacer `us-east-1` par l' Région AWS dans lequel vous avez créé vos propres compartiments source et de destination.

```
// dependencies
import { S3Client, GetObjectCommand, PutObjectCommand } from '@aws-sdk/client-
s3';

import { Readable } from 'stream';

import sharp from 'sharp';
import util from 'util';


// create S3 client
const s3 = new S3Client({region: 'us-east-1'});

// define the handler function
export const handler = async (event, context) => {

// Read options from the event parameter and get the source bucket
console.log("Reading options from event:\n", util.inspect(event, {depth: 5}));
  const srcBucket = event.Records[0].s3.bucket.name;

// Object key may have spaces or unicode non-ASCII characters
const srcKey    = decodeURIComponent(event.Records[0].s3.object.key.replace(/\+/
g, " "));
const dstBucket = srcBucket + "-resized";
const dstKey    = "resized-" + srcKey;

// Infer the image type from the file suffix
const typeMatch = srcKey.match(/\.([^.]*)$/);
if (!typeMatch) {
  console.log("Could not determine the image type.");
```

```
  return;
}

// Check that the image type is supported
const imageType = typeMatch[1].toLowerCase();
if (imageType != "jpg" && imageType != "png") {
  console.log(`Unsupported image type: ${imageType}`);
  return;
}

// Get the image from the source bucket. GetObjectCommand returns a stream.
try {
  const params = {
    Bucket: srcBucket,
    Key: srcKey
  };
  var response = await s3.send(new GetObjectCommand(params));
  var stream = response.Body;

// Convert stream to buffer to pass to sharp resize function.
  if (stream instanceof Readable) {
    var content_buffer = Buffer.concat(await stream.toArray());

  } else {
    throw new Error('Unknown object stream type');
  }


} catch (error) {
  console.log(error);
  return;
}


// set thumbnail width. Resize will set the height automatically to maintain
 aspect ratio.
const width  = 200;

// Use the sharp module to resize the image and save in a buffer.
try {
  var output_buffer = await sharp(content_buffer).resize(width).toBuffer();

} catch (error) {
  console.log(error);
```

```
  return;
}

// Upload the thumbnail image to the destination bucket
try {
  const destparams = {
    Bucket: dstBucket,
    Key: dstKey,
    Body: output_buffer,
    ContentType: "image"
  };

  const putResult = await s3.send(new PutObjectCommand(destparams));

  } catch (error) {
    console.log(error);
    return;
  }

  console.log('Successfully resized ' + srcBucket + '/' + srcKey +
    ' and uploaded to ' + dstBucket + '/' + dstKey);
  };
```

4. Dans votre répertoire `lambda-s3`, installez la bibliothèque sharp en utilisant npm. Notez que la dernière version de sharp (0.33) n'est pas compatible avec Lambda. Installez la version 0.32.6 pour terminer ce didacticiel.

```
npm install sharp@0.32.6
```

La commande npm `install` crée un répertoire `node_modules` pour vos modules. Après cette étape, votre structure de répertoire doit se présenter comme suit.

```
lambda-s3
|- index.mjs
|- node_modules
|  |- base64js
|  |- bl
|  |- buffer
...
|- package-lock.json
|- package.json
```

5. Créez un package de déploiement .zip contenant le code de votre fonction et ses dépendances. Sous macOS ou Linux, exécutez les commandes suivantes.

```
zip -r function.zip .
```

Sous Windows, utilisez l'utilitaire zip de votre choix pour créer un fichier .zip. Assurez-vous que vos fichiers `index.mjs`, `package.json`, et `package-lock.json` ainsi que votre répertoire `node_modules` se trouvent tous à la racine de votre fichier .zip.

Python

Pour créer le package de déploiement (Python)

1. Enregistrez l'exemple de code en tant que fichier nommé `lambda_function.py`.

```
import boto3
import os
import sys
import uuid
from urllib.parse import unquote_plus
from PIL import Image
import PIL.Image

s3_client = boto3.client('s3')

def resize_image(image_path, resized_path):
  with Image.open(image_path) as image:
    image.thumbnail(tuple(x / 2 for x in image.size))
    image.save(resized_path)

def lambda_handler(event, context):
  for record in event['Records']:
    bucket = record['s3']['bucket']['name']
    key = unquote_plus(record['s3']['object']['key'])
    tmpkey = key.replace('/', '')
    download_path = '/tmp/{}{}'.format(uuid.uuid4(), tmpkey)
    upload_path = '/tmp/resized-{}'.format(tmpkey)
    s3_client.download_file(bucket, key, download_path)
    resize_image(download_path, upload_path)
    s3_client.upload_file(upload_path, '{}-resized'.format(bucket), 'resized-
{}'.format(key))
```

2. Dans le même répertoire que celui dans lequel vous avez créé votre fichier `lambda_function.py`, créez un nouveau répertoire nommé `package` et installez la bibliothèque Pillow (PIL) et AWS SDK pour Python (Boto3). Bien que l'exécution Lambda Python inclut une version du kit SDK Boto3, nous vous recommandons d'ajouter toutes les dépendances de votre fonction à votre package de déploiement, même si elles sont incluses dans l'exécution. Pour plus d'informations, consultez la Dépendances d'exécution en Python.

   ```
   mkdir package
   pip install \
   --platform manylinux2014_x86_64 \
   --target=package \
   --implementation cp \
   --python-version 3.12 \
   --only-binary=:all: --upgrade \
   pillow boto3
   ```

   La bibliothèque Pillow contient le code C/C ++. À l'aide des `--only-binary=:all:` options `--platform manylinux_2014_x86_64` et, pip télécharge et installe une version de Pillow contenant des fichiers binaires précompilés compatibles avec le système d'exploitation Amazon Linux 2. Cela garantit que votre package de déploiement fonctionne dans l'environnement d'exécution Lambda, quels que soient le système d'exploitation et l'architecture de votre machine de construction locale.

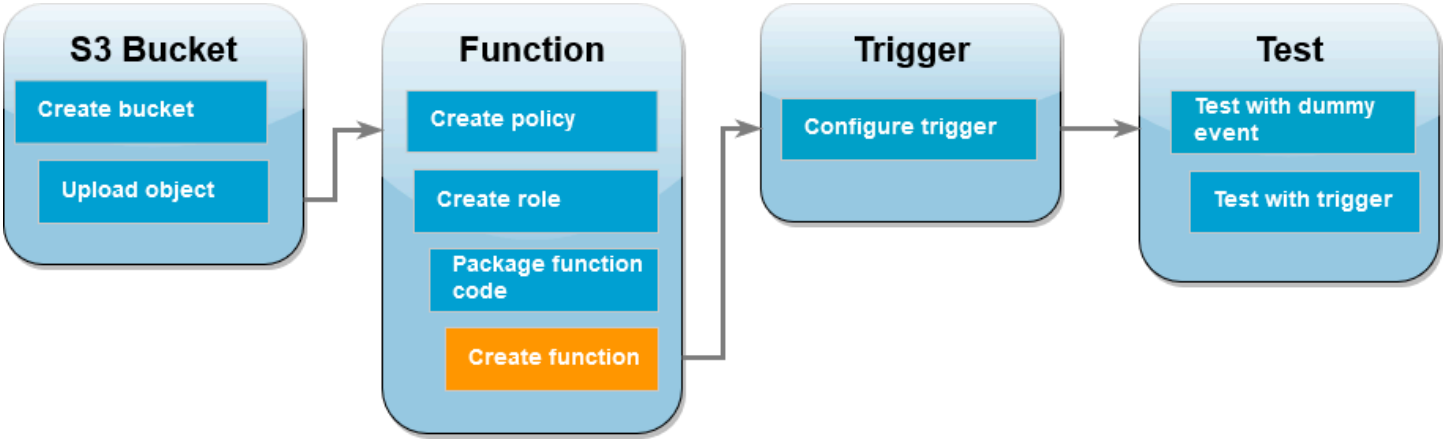
3. Créez un fichier .zip contenant le code de votre application et les bibliothèques Pillow et Boto3. Sous Linux ou macOS, exécutez les commandes suivantes depuis votre interface de ligne de commande.

   ```
   cd package
   zip -r ../lambda_function.zip .
   cd ..
   zip lambda_function.zip lambda_function.py
   ```

   Sous Windows, utilisez l'outil zip de votre choix pour créer le fichier `lambda_function.zip`. Assurez-vous que votre fichier `lambda_function.py` et les dossiers contenant vos dépendances sont installés à la racine du fichier .zip.

Vous pouvez également créer votre package de déploiement à l'aide d'un environnement virtuel Python. Consultez Utilisation d'archives de fichiers .zip pour les fonctions événementielles Lambda en Python

Création de la fonction d'événement Lambda



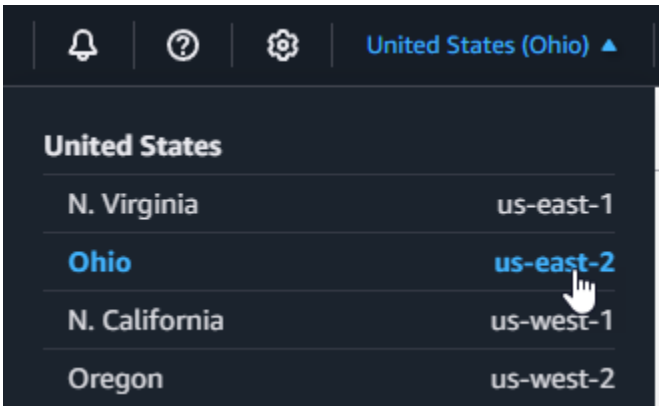
Vous pouvez créer votre fonction d'événement Lambda à l'aide de la console Lambda AWS CLI ou de la console Lambda. Suivez les instructions correspondant à la langue de votre choix pour créer la fonction.

Console de gestion AWS

Pour créer la fonction d'événement (console)

Pour créer votre fonction d'événement Lambda à l'aide de la console, vous devez d'abord créer une fonction de base contenant du code « Hello world ». Vous remplacez ensuite ce code par votre propre code de fonction en chargeant le fichier .zip ou JAR que vous avez créé à l'étape précédente.

1. Ouvrez la page Event Functions de la console Lambda.
2. Assurez-vous de travailler dans le même environnement que celui dans Région AWS lequel vous avez créé votre compartiment Amazon S3. Vous pouvez modifier votre région à l'aide de la liste déroulante en haut de l'écran.



3. Choisissez Create Event Function.

4. Choisissez Créer à partir de zéro.
5. Sous Informations de base, procédez comme suit :
   a. Sous Nom de la fonction, saisissez **`CreateThumbnail`**.
   b. Pour Runtime, choisissez Node.js 22.x ou Python 3.12 en fonction du langage que vous avez choisi pour votre fonction.
   c. Pour Architecture, choisissez x86_64.
6. Dans l'onglet Modifier le rôle d'exécution par défaut, procédez comme suit :
   a. Ouvrez l'onglet, puis choisissez Utiliser un rôle existant.
   b. Sélectionnez le `LambdaS3Role` que vous avez créé précédemment.
7. Choisissez Create Event Function.

Pour télécharger le code de la fonction d'événement (console)

1. Dans le volet Source du code, choisissez Charger à partir de.
2. Choisissez Fichier .zip.
3. Choisissez Charger.
4. Dans le sélecteur de fichiers, sélectionnez votre fichier .zip et choisissez Ouvrir.
5. Cliquez sur Enregistrer.

AWS CLI

Pour créer la fonction d'événement (AWS CLI)

- Exécutez la commande CLI pour la langue que vous avez choisie. Pour le `role` paramètre, assurez-vous de le remplacer `123456789012` par votre propre Compte AWS identifiant. Pour le paramètre `region`, remplacez `us-east-1` par la région dans laquelle vous avez créé vos compartiments Amazon S3.
  - Pour Node.js, exécutez la commande suivante depuis le répertoire contenant votre `function.zip` fichier.

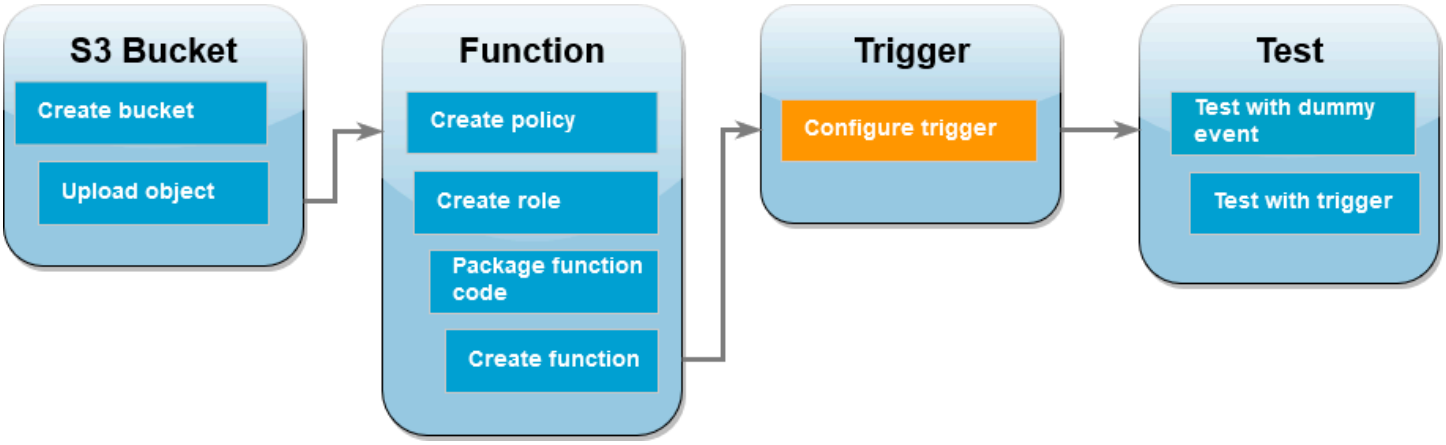
```
aws lambda create-function --function-name CreateThumbnail \
--zip-file fileb://function.zip --handler index.handler --runtime nodejs24.x \
--timeout 10 --memory-size 1024 \
```

```
--role arn:aws:iam::123456789012:role/LambdaS3Role --region us-east-1
```

- Pour Python, exécutez la commande suivante depuis le répertoire contenant votre fichier `lambda_function.zip`.

```
aws lambda create-function --function-name CreateThumbnail \
--zip-file fileb://lambda_function.zip --handler
 lambda_function.lambda_handler \
--runtime python3.14 --timeout 10 --memory-size 1024 \
--role arn:aws:iam::123456789012:role/LambdaS3Role --region us-east-1
```

Configurer Amazon S3 pour appeler la fonction d'événement



Pour que votre fonction d'événement Lambda s'exécute lorsque vous téléchargez une image dans votre compartiment source, vous devez configurer un déclencheur pour votre fonction. Vous pouvez configurer le déclencheur Amazon S3 à l'aide de la console ou de la AWS CLI.

> **Important**
>
> Cette procédure configure le compartiment Amazon S3 pour qu'il invoque votre fonction chaque fois qu'un objet est créé dans le compartiment. Veillez à configurer cela uniquement pour le compartiment source. Si votre fonction d'événement Lambda crée des objets dans le même compartiment que celui qui l'invoque, votre fonction peut être invoquée en continu dans une boucle. Cela peut entraîner la facturation de frais imprévus à votre Compte AWS charge.

Console de gestion AWS

Pour configurer le déclencheur Amazon S3 (console)

1. Ouvrez la page Event Functions de la console Lambda et choisissez votre fonction ()`CreateThumbnail`.
2. Choisissez Add trigger (Ajouter déclencheur).
3. Sélectionnez S3.
4. Sous Compartiment, sélectionnez votre compartiment source.
5. Sous Types d'événements, sélectionnez Tous les événements de création d'objets.
6. Sous Invocation récursive, cochez la case pour confirmer qu'il n'est pas recommandé d'utiliser le même compartiment Amazon S3 pour les entrées et les sorties. Vous pouvez en savoir plus sur les modèles d'invocation récursive dans Lambda en lisant la rubrique Modèles récursifs qui provoquent des fonctions Lambda incontrôlables dans Serverless Land.
7. Choisissez Ajouter.

   Lorsque vous créez un déclencheur à l'aide de la console Lambda, ce dernier crée automatiquement une politique basée sur une ressource pour donner au service que vous sélectionnez l'autorisation d'invoquer votre fonction.

AWS CLI

Pour configurer le déclencheur Amazon S3 (AWS CLI)

1. Pour que votre compartiment source Amazon S3 invoque votre fonction lorsque vous ajoutez un fichier image, vous devez d'abord configurer les autorisations pour votre fonction à l'aide d'une politique basée sur une ressource. Une déclaration de politique basée sur les ressources donne à d'autres personnes Services AWS l'autorisation d'invoquer votre fonction. Pour autoriser Amazon S3 à invoquer votre fonction, exécutez la commande CLI suivante. Assurez-vous de remplacer le `source-account` paramètre par votre propre Compte AWS identifiant et d'utiliser votre propre nom de compartiment source.

```
aws lambda add-permission --function-name CreateThumbnail \
--principal s3.amazonaws.com --statement-id s3invoke --action
 "lambda:InvokeFunction" \
--source-arn arn:aws:s3:::amzn-s3-demo-source-bucket \
--source-account 123456789012
```

La politique que vous définissez à l'aide de cette commande permet à Amazon S3 d'invoquer votre fonction uniquement lorsqu'une action a lieu sur votre compartiment source.

> **Note**
>
> Bien que les noms des compartiments Amazon S3 soient globalement uniques, il est préférable de spécifier que le compartiment doit appartenir à votre compte lorsque vous utilisez des politiques basées sur les ressources. En effet, si vous supprimez un bucket, il est possible qu'un autre Compte AWS en crée un avec le même Amazon Resource Name (ARN).

2. Enregistrez le JSON suivant dans un fichier nommé `notification.json`. Lorsqu'il est appliqué à votre compartiment source, ce JSON configure le compartiment pour envoyer une notification à votre fonction d'événement Lambda chaque fois qu'un nouvel objet est ajouté. Remplacez le Compte AWS numéro et Région AWS dans l'ARN de la fonction d'événement Lambda par votre propre numéro de compte et votre propre région.

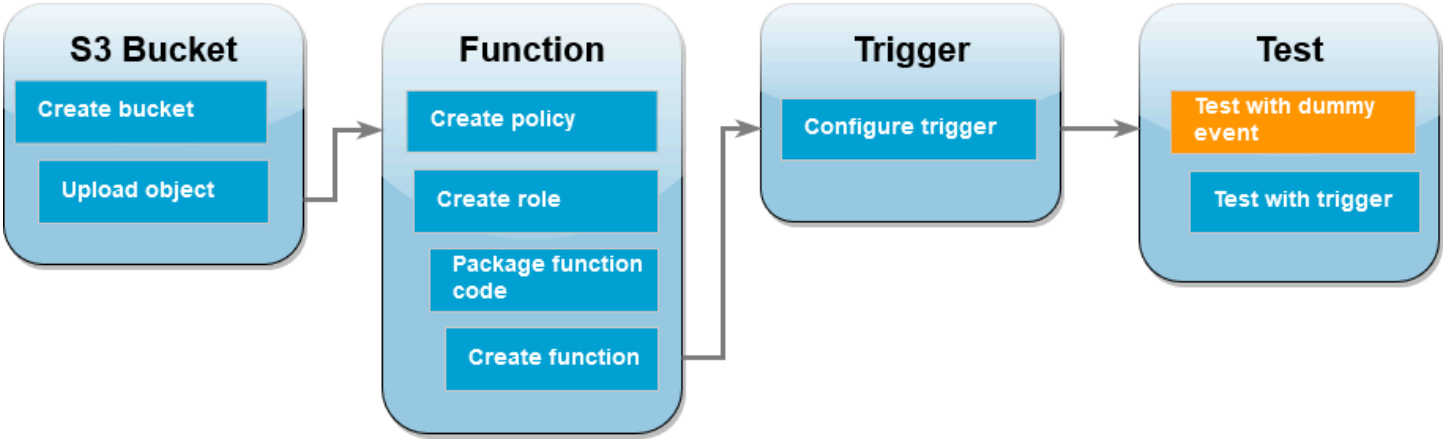
```
{
"LambdaFunctionConfigurations": [
    {
      "Id": "CreateThumbnailEventConfiguration",
      "LambdaFunctionArn": "arn:aws:lambda:us-
east-1:123456789012:function:CreateThumbnail",
      "Events": [ "s3:ObjectCreated:Put" ]
    }
  ]
}
```

3. Exécutez la commande CLI suivante pour appliquer les paramètres de notification du fichier JSON que vous avez créé à votre compartiment source. Remplacez `amzn-s3-demo-source-bucket` par le nom de votre propre compartiment source.

```
aws s3api put-bucket-notification-configuration --bucket amzn-s3-demo-source-
bucket \
--notification-configuration file://notification.json
```

Pour en savoir plus sur la commande `put-bucket-notification-configuration` et l'option `notification-configuration`, consultez la section put-bucket-notification-configuration dans la référence des commandes de la CLI AWS .

Testez votre fonction d'événement Lambda avec un événement factice



Avant de tester l'ensemble de votre configuration en ajoutant un fichier image à votre compartiment source Amazon S3, vous devez vérifier que votre fonction d'événement Lambda fonctionne correctement en l'invoquant avec un événement factice. Dans Lambda, un événement est un JSON-formatted document qui contient des données que votre fonction doit traiter. Lorsque votre fonction est invoquée par Amazon S3, l'événement envoyé à votre fonction contient des informations telles que le nom du compartiment, l'ARN du compartiment et la clé de l'objet.

Console de gestion AWS

Pour tester votre fonction d'événement Lambda avec un événement factice (console)

1. Ouvrez la page Event Functions de la console Lambda et choisissez votre fonction ()`CreateThumbnail`.
2. Choisissez l'onglet Test.
3. Pour créer votre événement de test, dans le volet Événement de test, procédez comme suit :
   a. Sous Action d'événement de test, sélectionnez Créer un nouvel événement.
   b. Dans Event name (Nom de l'événement), saisissez **`myTestEvent`**.
   c. Pour Modèle, sélectionnez S3 Put.
   d. Remplacez les valeurs des paramètres suivants par vos propres valeurs.
      - Pour`awsRegion`, remplacez-le `us-east-1` par celui dans Région AWS lequel vous avez créé vos compartiments Amazon S3.
      - Pour `name`, remplacez `amzn-s3-demo-bucket` par le nom de votre propre compartiment source Amazon S3.

- Pour `key`, remplacez `test%2Fkey` par le nom de fichier de l'objet de test que vous avez chargé dans votre compartiment source à l'étape Charger une image de test dans votre compartiment source.

```
{
  "Records": [
    {
      "eventVersion": "2.0",
      "eventSource": "aws:s3",
      "awsRegion": "us-east-1",
      "eventTime": "1970-01-01T00:00:00.000Z",
      "eventName": "ObjectCreated:Put",
      "userIdentity": {
        "principalId": "EXAMPLE"
      },
      "requestParameters": {
        "sourceIPAddress": "127.0.0.1"
      },
      "responseElements": {
        "x-amz-request-id": "EXAMPLE123456789",
        "x-amz-id-2": "EXAMPLE123/5678abcdefghijklambdaisawesome/
mnopqrstuvwxyzABCDEFGH"
      },
      "s3": {
        "s3SchemaVersion": "1.0",
        "configurationId": "testConfigRule",
        "bucket": {
          "name": "amzn-s3-demo-bucket",
          "ownerIdentity": {
            "principalId": "EXAMPLE"
          },
          "arn": "arn:aws:s3:::amzn-s3-demo-bucket"
        },
        "object": {
          "key": "test%2Fkey",
          "size": 1024,
          "eTag": "0123456789abcdef0123456789abcdef",
          "sequencer": "0A1B2C3D4E5F678901"
        }
      }
    }
  ]
```

```
}
```

e. Cliquez sur Enregistrer.

4. Dans le volet Événement de test, choisissez Test.
5. Pour vérifier que votre fonction a créé une version redimensionnée de votre image et l'a stockée dans votre compartiment Amazon S3 cible, procédez comme suit :

   a. Ouvrez la page Compartiments de la console Amazon S3.

   b. Choisissez votre compartiment cible et vérifiez que votre fichier redimensionné est répertorié dans le volet Objets.

AWS CLI

Pour tester votre fonction d'événement Lambda avec un événement factice (AWS CLI)

1. Enregistrez le JSON suivant dans un fichier nommé `dummyS3Event.json`. Remplacez les valeurs des paramètres suivants par vos propres valeurs :

   - Pour `awsRegion`, remplacez-le `us-east-1` par celui dans Région AWS lequel vous avez créé vos compartiments Amazon S3.
   - Pour `name`, remplacez `amzn-s3-demo-bucket` par le nom de votre propre compartiment source Amazon S3.
   - Pour `key`, remplacez `test%2Fkey` par le nom de fichier de l'objet de test que vous avez chargé dans votre compartiment source à l'étape Charger une image de test dans votre compartiment source.

```
{
  "Records": [
    {
      "eventVersion": "2.0",
      "eventSource": "aws:s3",
      "awsRegion": "us-east-1",
      "eventTime": "1970-01-01T00:00:00.000Z",
      "eventName": "ObjectCreated:Put",
      "userIdentity": {
        "principalId": "EXAMPLE"
      },
      "requestParameters": {
```

```
        "sourceIPAddress": "127.0.0.1"
      },
      "responseElements": {
        "x-amz-request-id": "EXAMPLE123456789",
        "x-amz-id-2": "EXAMPLE123/5678abcdefghijklambdaisawesome/
mnopqrstuvwxyzABCDEFGH"
      },
      "s3": {
        "s3SchemaVersion": "1.0",
        "configurationId": "testConfigRule",
        "bucket": {
          "name": "amzn-s3-demo-bucket",
          "ownerIdentity": {
            "principalId": "EXAMPLE"
          },
          "arn": "arn:aws:s3:::amzn-s3-demo-bucket"
        },
        "object": {
          "key": "test%2Fkey",
          "size": 1024,
          "eTag": "0123456789abcdef0123456789abcdef",
          "sequencer": "0A1B2C3D4E5F678901"
        }
      }
    }
  ]
}
```

2. À partir du répertoire dans lequel vous avez enregistré votre fichier dummyS3Event.json, invoquez la fonction en exécutant la commande CLI suivante. Cette commande appelle votre fonction d'événement Lambda de manière synchrone en RequestResponse spécifiant comme valeur le paramètre de type d'appel. Pour en savoir plus sur l'invocation synchrone et asynchrone, consultez Invocation de fonctions Lambda.

```
aws lambda invoke --function-name CreateThumbnail \
--invocation-type RequestResponse --cli-binary-format raw-in-base64-out \
--payload file://dummyS3Event.json outputfile.txt
```

L'option cli-binary-format est obligatoire si vous utilisez la version 2 de la AWS CLI. Pour faire de ce paramètre le paramètre par défaut, exécutez aws configure set cli-binary-format raw-in-base64-out. Pour plus d'informations, veuillez consulter les AWS CLI options de ligne de commande.

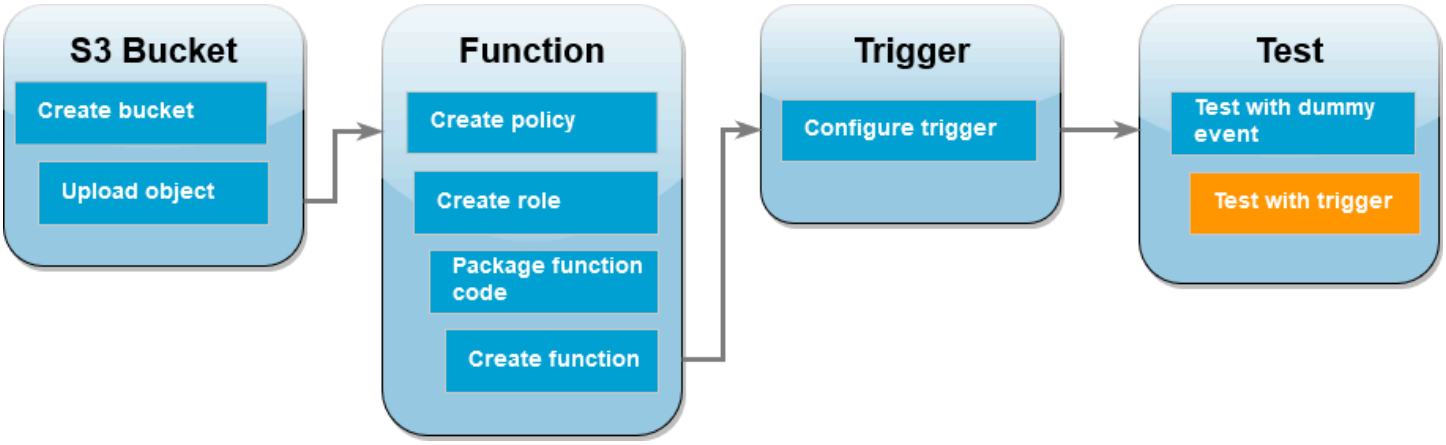
3. Vérifiez que votre fonction a créé une version miniature de votre image et l'a enregistrée dans votre compartiment Amazon S3 cible. Exécutez la commande CLI suivante, en remplaçant `amzn-s3-demo-source-bucket-resized` par le nom de votre compartiment de destination.

```
aws s3api list-objects-v2 --bucket amzn-s3-demo-source-bucket-resized
```

Vous devez visualiser des résultats similaires à ce qui suit. Le paramètre `Key` indique le nom de fichier de votre fichier image redimensionné.

```
{
    "Contents": [
        {
            "Key": "resized-HappyFace.jpg",
            "LastModified": "2023-06-06T21:40:07+00:00",
            "ETag": "\"d8ca652ffe83ba6b721ffc20d9d7174a\"",
            "Size": 2633,
            "StorageClass": "STANDARD"
        }
    ]
}
```

Testez votre fonction d'événement à l'aide du déclencheur Amazon S3



Maintenant que vous avez confirmé que votre fonction d'événement Lambda fonctionne correctement, vous êtes prêt à tester l'ensemble de votre configuration en ajoutant un fichier image à votre compartiment source Amazon S3. Lorsque vous ajoutez votre image au compartiment source,

votre fonction d'événement Lambda doit être automatiquement invoquée. Votre fonction crée une version redimensionnée du fichier et la stocke dans votre compartiment cible.

Console de gestion AWS

Pour tester votre fonction d'événement Lambda à l'aide du déclencheur Amazon S3 (console)

1. Pour charger une image dans votre compartiment Amazon S3, procédez comme suit :
   a. Ouvrez la page Compartiments de la console Amazon S3 et choisissez votre compartiment source.
   b. Choisissez Charger.
   c. Choisissez Ajouter des fichiers et utilisez le sélecteur de fichiers pour sélectionner le fichier image que vous souhaitez charger. Votre objet image peut être n'importe quel fichier .jpg ou .png.
   d. Choisissez Ouvrir, puis Charger.
2. Vérifiez que Lambda a enregistré une version redimensionnée de votre fichier image dans votre compartiment cible en procédant comme suit :
   a. Retournez à la page Compartiments de la console Amazon S3 et choisissez votre compartiment de destination.
   b. Dans le volet Objets, vous devriez maintenant voir deux fichiers image redimensionnés, un pour chaque test de votre fonction d'événement Lambda. Pour télécharger votre image redimensionnée, sélectionnez le fichier, puis choisissez Télécharger.

AWS CLI

Pour tester votre fonction d'événement Lambda à l'aide du déclencheur Amazon S3 (AWS CLI)

1. À partir du répertoire contenant l'image que vous souhaitez charger, exécutez la commande CLI suivante. Remplacez le paramètre `--bucket` par le nom de votre compartiment source. Pour les paramètres `--key` et `--body`, utilisez le nom de fichier de votre image de test. Votre image de test peut être n'importe quel fichier .jpg ou .png.

```
aws s3api put-object --bucket amzn-s3-demo-source-bucket --key SmileyFace.jpg --
body ./SmileyFace.jpg
```

2. Vérifiez que votre fonction a créé une version miniature de votre image et l'a enregistrée dans votre compartiment Amazon S3 cible. Exécutez la commande CLI suivante, en remplaçant `amzn-s3-demo-source-bucket-resized` par le nom de votre compartiment de destination.

```
aws s3api list-objects-v2 --bucket amzn-s3-demo-source-bucket-resized
```

Si votre fonction s'exécute correctement, vous obtiendrez un résultat similaire à ce qui suit. Votre compartiment cible doit désormais contenir deux fichiers redimensionnés.

```
{
    "Contents": [
        {
            "Key": "resized-HappyFace.jpg",
            "LastModified": "2023-06-07T00:15:50+00:00",
            "ETag": "\"7781a43e765a8301713f533d70968a1e\"",
            "Size": 2763,
            "StorageClass": "STANDARD"
        },
        {
            "Key": "resized-SmileyFace.jpg",
            "LastModified": "2023-06-07T00:13:18+00:00",
            "ETag": "\"ca536e5a1b9e32b22cd549e18792cdbc\"",
            "Size": 1245,
            "StorageClass": "STANDARD"
        }
    ]
}
```

Nettoyage de vos ressources

Vous pouvez maintenant supprimer les ressources que vous avez créées pour ce didacticiel, sauf si vous souhaitez les conserver. En supprimant AWS les ressources que vous n'utilisez plus, vous évitez des frais inutiles pour votre Compte AWS.

Pour supprimer la fonction d'événement Lambda

1. Ouvrez la page Event Functions de la console Lambda.
2. Sélectionnez la fonction d'événement que vous avez créée.

3. Sélectionnez Actions, Supprimer.
4. Saisissez **`confirm`** dans la zone de saisie de texte et choisissez Delete (Supprimer).

Suppression de la stratégie que vous avez créée

1. Ouvrez la page Policies (Politiques) de la console IAM.
2. Sélectionnez la politique que vous avez créée (AWSLambdaS3Policy).
3. Choisissez Actions de stratégie, Supprimer.
4. Sélectionnez Supprimer.

Pour supprimer le rôle d'exécution

1. Ouvrez la page Roles (Rôles) de la console IAM.
2. Sélectionnez le rôle d'exécution que vous avez créé.
3. Sélectionnez Supprimer.
4. Saisissez le nom du rôle dans le champ de saisie de texte et choisissez Delete (Supprimer).

Pour supprimer le compartiment S3

1. Ouvrez la console Amazon S3.
2. Sélectionnez le compartiment que vous avez créé.
3. Sélectionnez Supprimer.
4. Saisissez le nom du compartiment dans le champ de saisie de texte.
5. Choisissez Supprimer le compartiment.

Utiliser les secrets de Secrets Manager dans Lambda Event Functions

AWS Secrets Manager vous aide à gérer les informations d'identification, les clés d'API et les autres secrets dont vos fonctions d'événement Lambda ont besoin. Vous disposez de deux approches principales pour récupérer des secrets dans vos fonctions d'événement Lambda, toutes deux offrant de meilleures performances et des coûts réduits par rapport à la récupération de secrets directement à l'aide du SDK : AWS

- AWS paramètres et secrets Extension Lambda : solution indépendante de l'exécution qui fournit une interface HTTP simple pour récupérer les secrets
- Utilitaire Powertools for AWS Lambda Parameters : solution intégrée au code qui prend en charge plusieurs fournisseurs (Secrets Manager, Parameter Store AppConfig) avec des transformations intégrées

Les deux approches conservent des caches locaux de secrets, ce qui évite à votre fonction d’appeler Secrets Manager pour chaque invocation. Lorsque votre fonction demande un secret, le cache est d’abord vérifié. Si le secret est disponible et n’a pas expiré, il est renvoyé immédiatement. Sinon, il est extrait de Secrets Manager, mis en cache et renvoyé. Ce mécanisme de mise en cache permet d’accélérer les temps de réponse et de réduire les coûts en minimisant les appels d’API.

Choix d’une approche

Tenez compte des facteurs suivants lorsque vous choisissez entre l'extension et PowerTools :

Utilisez l'extension Lambda de AWS paramètres et de secrets lorsque :

- Vous recherchez une solution indépendante de l’environnement d’exécution qui fonctionne avec n’importe quel environnement d’exécution Lambda
- Vous préférez ne pas ajouter de dépendances de code à votre fonction
- Vous souhaitez seulement récupérer des secrets à partir de Secrets Manager ou de Parameter Store

Utilisez Powertools pour l'utilitaire AWS Lambda de paramètres lorsque :

- Vous souhaitez bénéficier d’une expérience de développement intégrée au code de votre application
- Vous avez besoin d'assistance pour plusieurs fournisseurs (Secrets Manager, Parameter Store, AppConfig)
- Vous souhaitez des transformations de données intégrées (analyse JSON, décodage Base64)

- Vous utilisez des environnements d'exécution Python TypeScript, Java ou .NET

Quand utiliser Secrets Manager avec Lambda

Les scénarios courants d’utilisation de Secrets Manager avec Lambda comprennent les suivants :

- Stockage d’informations d’identification de base de données que votre fonction utilise pour se connecter à Amazon RDS ou d’autres bases de données
- Gestion des clés d’API pour les services externes appelés par votre fonction
- Stockage des clés de chiffrement ou d’autres données de configuration sensibles
- Rotation automatique des informations d’identification sans qu’il soit nécessaire de mettre à jour le code de votre fonction

Utilisation de AWS paramètres et secrets Extension Lambda

L'extension Lambda de AWS paramètres et de secrets utilise une interface HTTP simple compatible avec n'importe quel environnement d'exécution Lambda. Par défaut, elle met en cache les secrets pendant 300 secondes (5 minutes) et peut contenir jusqu’à 1 000 secrets. Vous pouvez personnaliser ces paramètres à l’aide de variables d’environnement.

Utiliser Secrets Manager dans une fonction d'événement Lambda

Cette section part du principe que vous possédez déjà un secret Secrets Manager. Pour créer un secret, voir Création d'un AWS Secrets Manager secret.

Création du package de déploiement

Choisissez votre environnement d’exécution préféré et suivez les étapes pour créer une fonction qui récupère les secrets depuis Secrets Manager. L’exemple de fonction extrait un secret dans Secrets Manager et peut être utilisé pour accéder aux informations d’identification de base de données, aux clés d’API ou à d’autres données de configuration sensibles dans vos applications.

Python

Pour créer une fonction d'événement Python

1. Créez et accédez à un nouveau répertoire de projet. Exemple :

```
mkdir my_function
```

```
cd my_function
```

2. Créez un fichier nommé `lambda_function.py` avec le code suivant. Pour `secret_name`, utilisez le nom ou l'Amazon Resource Name (ARN) de votre secret.

```
import json
import boto3
import requests

def lambda_handler(event, context):
    try:
        # Replace with the name or ARN of your secret
        secret_name = "arn:aws:secretsmanager:us-
east-1:111122223333:secret:SECRET_NAME"

        # Resolve the session token from the credential provider chain so that
 this
        # works across all initialization modes, including SnapStart. Resolve
 inside
        # the handler so the token stays fresh after a SnapStart restore.
        session_token =
 boto3.Session().get_credentials().get_frozen_credentials().token

        secrets_extension_endpoint = f"http://localhost:2773/secretsmanager/get?
secretId={secret_name}"
        headers = {"X-Aws-Parameters-Secrets-Token": session_token}

        response = requests.get(secrets_extension_endpoint, headers=headers)
        print(f"Response status code: {response.status_code}")

        secret = json.loads(response.text)["SecretString"]
        print(f"Retrieved secret: {secret}")

        return {
            'statusCode': response.status_code,
            'body': json.dumps({
                'message': 'Successfully retrieved secret',
                'secretRetrieved': True
            })
        }

    except Exception as e:
        print(f"Error: {str(e)}")
```

```
        return {
            'statusCode': 500,
            'body': json.dumps({
                'message': 'Error retrieving secret',
                'error': str(e)
            })
        }
```

3. Créez un fichier nommé `requirements.txt` avec ce contenu :

```
requests
```

4. Installez les dépendances :

```
pip install -r requirements.txt -t .
```

5. Créez un fichier .zip contenant tous les fichiers :

```
zip -r function.zip .
```

Node.js

Pour créer une fonction Node.js d'événement

1. Créez et accédez à un nouveau répertoire de projet. Exemple :

```
mkdir my_function
cd my_function
```

2. Créez un fichier nommé `index.mjs` avec le code suivant. Pour `secret_name`, utilisez le nom ou l'Amazon Resource Name (ARN) de votre secret.

```
import http from 'http';
import { fromNodeProviderChain } from '@aws-sdk/credential-providers';

export const handler = async (event) => {
    try {
        // Replace with the name or ARN of your secret
        const secretName = "arn:aws:secretsmanager:us-
east-1:111122223333:secret:SECRET_NAME";
```

```
        // Resolve the session token from the credential provider chain so that
this
        // works across all initialization modes, including SnapStart. Resolve
inside
        // the handler so the token stays fresh after a SnapStart restore.
        const { sessionToken } = await fromNodeProviderChain()();

        const options = {
            hostname: 'localhost',
            port: 2773,
            path: `/secretsmanager/get?secretId=${secretName}`,
            headers: {
                'X-Aws-Parameters-Secrets-Token': sessionToken
            }
        };

        const response = await new Promise((resolve, reject) => {
            http.get(options, (res) => {
                let data = '';
                res.on('data', (chunk) => { data += chunk; });
                res.on('end', () => {
                    resolve({
                        statusCode: res.statusCode,
                        body: data
                    });
                });
            }).on('error', reject);
        });

        const secret = JSON.parse(response.body).SecretString;
        console.log('Retrieved secret:', secret);

        return {
            statusCode: response.statusCode,
            body: JSON.stringify({
                message: 'Successfully retrieved secret',
                secretRetrieved: true
            })
        };
    } catch (error) {
        console.error('Error:', error);
        return {
            statusCode: 500,
            body: JSON.stringify({
```

```
                message: 'Error retrieving secret',
                error: error.message
            })
        };
    }
};
```

3. Créez un fichier .zip contient le fichier `index.mjs`.

```
zip -r function.zip index.mjs
```

Java

Pour créer une fonction d'événement Java

1. Créez un projet Maven :

```
mvn archetype:generate \
    -DgroupId=example \
    -DartifactId=lambda-secrets-demo \
    -DarchetypeArtifactId=maven-archetype-quickstart \
    -DarchetypeVersion=1.4 \
    -DinteractiveMode=false
```

2. Accédez au répertoire du projet :

```
cd lambda-secrets-demo
```

3. Ouvrez `pom.xml` et remplacez le contenu par ce qui suit :

```
<project xmlns="http://maven.apache.org/POM/4.0.0"
         xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
         xsi:schemaLocation="http://maven.apache.org/POM/4.0.0 http://
maven.apache.org/xsd/maven-4.0.0.xsd">
    <modelVersion>4.0.0</modelVersion>

    <groupId>example</groupId>
    <artifactId>lambda-secrets-demo</artifactId>
    <version>1.0-SNAPSHOT</version>

    <properties>
        <maven.compiler.source>11</maven.compiler.source>
```

```
        <maven.compiler.target>11</maven.compiler.target>
    </properties>

    <dependencies>
        <dependency>
            <groupId>com.amazonaws</groupId>
            <artifactId>aws-lambda-java-core</artifactId>
            <version>1.2.1</version>
        </dependency>
        <dependency>
            <groupId>software.amazon.awssdk</groupId>
            <artifactId>auth</artifactId>
            <version>2.25.0</version>
        </dependency>
    </dependencies>

    <build>
        <plugins>
            <plugin>
                <groupId>org.apache.maven.plugins</groupId>
                <artifactId>maven-shade-plugin</artifactId>
                <version>3.2.4</version>
                <executions>
                    <execution>
                        <phase>package</phase>
                        <goals>
                            <goal>shade</goal>
                        </goals>
                        <configuration>
                            <createDependencyReducedPom>false</
createDependencyReducedPom>
                            <finalName>function</finalName>
                        </configuration>
                    </execution>
                </executions>
            </plugin>
        </plugins>
    </build>
</project>
```

4. Renommez `/lambda-secrets-demo/src/main/java/example/App.java` en `Hello.java` pour qu'il corresponde au nom du gestionnaire Java par défaut de Lambda (`example.Hello::handleRequest`) :

```
mv src/main/java/example/App.java src/main/java/example/Hello.java
```

5. Ouvrez le fichier `Hello.java` et remplacez son contenu par ce qui suit. Pour `secretName`, utilisez le nom ou l'Amazon Resource Name (ARN) de votre secret.

```
package example;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import software.amazon.awssdk.auth.credentials.DefaultCredentialsProvider;
import software.amazon.awssdk.auth.credentials.AwsSessionCredentials;
import java.net.URI;
import java.net.http.HttpClient;
import java.net.http.HttpRequest;
import java.net.http.HttpResponse;

public class Hello implements RequestHandler<Object, String> {
    private final HttpClient client = HttpClient.newHttpClient();
    private final DefaultCredentialsProvider credentialsProvider =
 DefaultCredentialsProvider.create();

    @Override
    public String handleRequest(Object input, Context context) {
        try {
            // Replace with the name or ARN of your secret
            String secretName = "arn:aws:secretsmanager:us-
east-1:111122223333:secret:SECRET_NAME";
            String endpoint = "http://localhost:2773/secretsmanager/get?
secretId=" + secretName;

            // Resolve the session token from the credential provider chain so
 that this
            // works across all initialization modes, including SnapStart.
 Resolve inside
            // the handler so the token stays fresh after a SnapStart restore.
            AwsSessionCredentials credentials = (AwsSessionCredentials)
 credentialsProvider.resolveCredentials();
            String sessionToken = credentials.sessionToken();

            HttpRequest request = HttpRequest.newBuilder()
                .uri(URI.create(endpoint))
                .header("X-Aws-Parameters-Secrets-Token", sessionToken)
```

```
                .GET()
                .build();

            HttpResponse<String> response = client.send(request,
                HttpResponse.BodyHandlers.ofString());

            String secret = response.body();
            secret = secret.substring(secret.indexOf("SecretString") + 15);
            secret = secret.substring(0, secret.indexOf("\""));

            System.out.println("Retrieved secret: " + secret);
            return String.format(
                "{\"statusCode\": %d, \"body\": \"%s\"}",
                response.statusCode(), "Successfully retrieved secret"
            );

        } catch (Exception e) {
            e.printStackTrace();
            return String.format(
                "{\"body\": \"Error retrieving secret: %s\"}",
                e.getMessage()
            );
        }
    }
}
```

6. Supprimez le répertoire de test. Maven le crée par défaut, mais nous n'en avons pas besoin pour cet exemple.

```
rm -rf src/test
```

7. Générez le projet :

```
mvn package
```

8. Téléchargez le fichier JAR (`target/function.jar`) pour une utilisation ultérieure.

Création de la fonction d'événement

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez Create Event Function.
3. Sélectionnez Créer à partir de zéro.

4. Sous Nom de la fonction, saisissez **`secret-retrieval-demo`**.
5. Choisissez votre Environnement d'exécution préféré.
6. Choisissez Create Event Function.

Charger un package de déploiement

1. Dans l'onglet Code de la fonction, choisissez Upload from et sélectionnez le fichier .zip (pour Python et Node.js) ou le fichier .jar (pour Java).
2. Chargez le package de déploiement créé précédemment.
3. Cliquez sur Enregistrer.

Ajouter l'extension

Pour ajouter le AWS Paramètres et secrets Extension Lambda en tant que couche

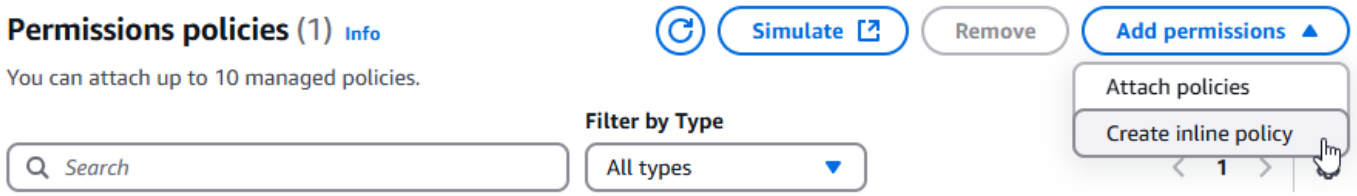
1. Dans l'onglet Code de la fonction, faites défiler la page jusqu'à Couches.
2. Choisissez Add a layer (Ajouter une couche).
3. Sélectionnez Couches AWS .
4. Choisissez AWS- Parameters-and-Secrets-Lambda-Extension.
5. Sélectionnez la dernière version.
6. Choisissez Ajouter.

Ajout d'autorisations

Ajouter des autorisations Secrets Manager à votre rôle d'exécution

1. Choisissez l'onglet Configuration, puis Permissions (Autorisations).
2. Sous Nom du rôle, cliquez sur le lien vers votre rôle d'exécution. Ce lien ouvre le rôle dans la console IAM.

3. Sélectionnez Ajouter des autorisations, puis Ajouter la politique.



4. Choisissez l'onglet JSON et ajoutez la politique suivante. Pour `Resource`, saisissez l'ARN de votre secret.

   JSON

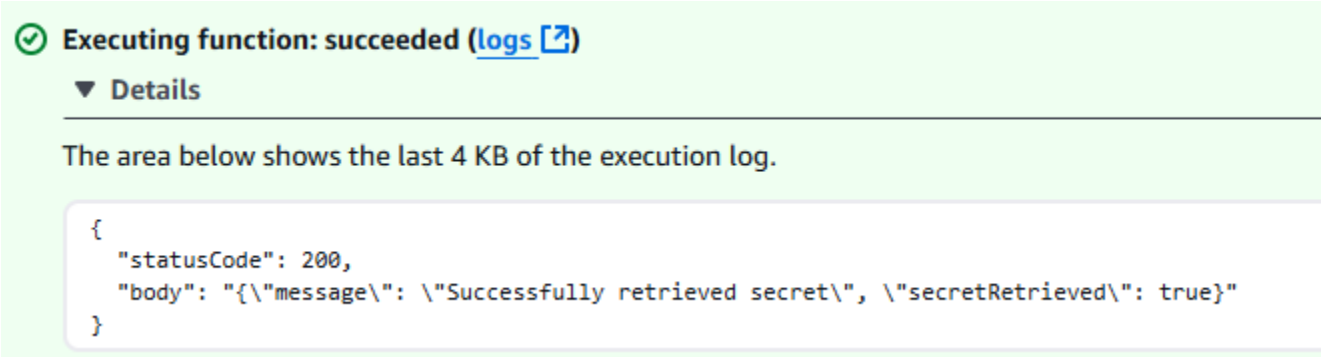
```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "secretsmanager:GetSecretValue",
            "Resource": "arn:aws:secretsmanager:us-
east-1:111122223333:secret:SECRET_NAME"
        }
    ]
}
```

5. Choisissez Suivant.
6. Entrez le nom de la politique.
7. Choisissez Create Policy (Créer une politique).

Tester la fonction d'événement

Pour tester la fonction d'événement

1. Retournez à la console Lambda.
2. Sélectionnez l'onglet Test.
3. Sélectionnez Tester). Vous devriez voir la réponse suivante :



Variables d’environnement

L'extension Lambda AWS Parameters and Secrets utilise les paramètres par défaut suivants. Vous pouvez remplacer ces paramètres en créant les variables d’environnement correspondantes. Pour afficher les paramètres actuels d’une fonction, réglez `PARAMETERS_SECRETS_EXTENSION_LOG_LEVEL` sur `DEBUG`. L'extension enregistre ses informations de configuration dans CloudWatch Logs au début de chaque appel de fonction.

Paramètre	Valeur par défaut	Valeurs valides	Variable d'environnement	Détails
Port HTTP	2773	1 – 65535	PARAMETERS_SECRETS_EXTENSION_HTTP_PORT	Port du serveur HTTP local
Cache activé	TRUE	TRUE | FALSE	PARAMETERS_SECRETS_EXTENSION_CACHE_ENABLED	Activer ou désactiver le cache
Taille du cache	1 000	0 - 1000	PARAMETERS_SECRETS_EXTENSION_CACHE_SIZE	Définissez cette valeur sur 0 pour désactiver la mise en cache
TTL de Secrets Manager	300 seconde	0 à 300 seconde	SECRETS_MANAGER_TTL	Time-to-live pour les secrets mis en cache. Définissez sur 0 pour désactiver la mise en cache. Cette variable est ignorée si la valeur

Paramètre	Valeur par défaut	Valeurs valides	Variable d'environnement	Détails
				de PARAMETER S_SECRETS_EXTENSIO N_CACHE_SIZE est de 0.
TTL du magasin de paramètres	300 seconde	0 à 300 seconde	SSM_PARAM ETER_STORE_TTL	Time-to-live pour les paramètres mis en cache. Définissez sur 0 pour désactiver la mise en cache. Cette variable est ignorée si la valeur de PARAMETER S_SECRETS_EXTENSIO N_CACHE_SIZE est de 0.
Niveau de journalis ation	INFO	DEBUG | INFO | WARN | ERROR | NONE	PARAMETER S_SECRETS_EXTENSIO N_LOG_LEVEL	Le niveau de détail indiqué dans les journaux pour l’extension
Nombre maximal de connexions	3	1 ou plus	PARAMETER S_SECRETS_EXTENSIO N_MAX_CONNECTIONS	Nombre maximum de connexions HTTP pour les requêtes à Parameter Store ou Secrets Manager.
Délai d’expiration de Secrets Manager	0 (n’expire pas)	Tous les nombres entiers	SECRETS_M ANAGER_TIMEOUT_MIL LIS	Délai d’expiration des requêtes adressées à Secrets Manager (en millisecondes)

Paramètre	Valeur par défaut	Valeurs valides	Variable d'environnement	Détails
Délai d'expiration de Parameter Store	0 (n'expire pas)	Tous les nombres entiers	SSM_PARAMETER_STORE_TIMEOUT_MILLIS	Délai d'expiration des requêtes adressées au Parameter Store (en millisecondes)

Utilisation d'une rotation des secrets

Si vous alternez fréquemment les secrets, la durée de cache par défaut de 300 secondes peut entraîner l'utilisation de secrets obsolètes par votre fonction. Deux options s'offrent à vous pour vous assurer que votre fonction utilise la dernière valeur de secret :

- Réduisez le TTL du cache en définissant la variable d'environnement `SECRETS_MANAGER_TTL` sur une valeur inférieure (en secondes). Par exemple, configurez-le sur `60` pour que votre fonction n'utilise jamais un secret vieux de plus d'une minute.
- Utilisez les étiquettes intermédiaires `AWSCURRENT` ou `AWSPREVIOUS` dans votre demande de secret pour vous assurer d'obtenir la version spécifique que vous souhaitez :

```
secretsmanager/get?secretId=YOUR_SECRET_NAME&versionStage=AWSCURRENT
```

Choisissez l'approche qui équilibre le mieux vos besoins en matière de performances et de fraîcheur. Un TTL inférieur signifie des appels plus fréquents à Secrets Manager, mais garantit que vous travaillez avec les valeurs de secret les plus récentes.

Utilisation de l'utilitaire de paramètres de Powertools pour AWS Lambda

L'utilitaire de paramètres de Powertools for AWS Lambda fournit une interface unifiée permettant de récupérer les secrets auprès de plusieurs fournisseurs, notamment Secrets Manager, le magasin de paramètres et. AppConfig Il gère la mise en cache, les transformations et fournit une expérience de développement plus intégrée par rapport à l'approche de l'extension.

Avantages de l’utilitaire de paramètres

- Fournisseurs multiples - Récupérez les paramètres depuis Secrets Manager, Parameter Store et AppConfig en utilisant la même interface
- Built-in transformations - Analyse automatique JSON, décodage base64 et autres transformations de données
- Mise en cache intégrée : mise en cache configurable avec prise en charge de TTL pour réduire les appels d’API
- Sécurité typographique : prise en charge efficace de la saisie dans les environnements d'exécution compatibles TypeScript et dans les autres environnements d'exécution compatibles
- Gestion des erreurs : logique Built-in des nouvelles tentatives et gestion des erreurs

Exemples de code

Les exemples suivants montrent comment récupérer des secrets à l’aide de l’utilitaire de paramètres dans différents environnements d’exécution :

Python

> **Note**
>
> Pour obtenir des exemples complets et des instructions de configuration, consultez la documentation de l’utilitaire de paramètres.

Récupération de secrets depuis Secrets Manager avec l'utilitaire Powertools for AWS Lambda Parameters.

```
from aws_lambda_powertools import Logger
from aws_lambda_powertools.utilities import parameters

logger = Logger()

def lambda_handler(event, context):
    try:
        # Get secret with caching (default TTL: 5 seconds)
        secret_value = parameters.get_secret("my-secret-name")

        # Get secret with custom TTL
```

```
        secret_with_ttl = parameters.get_secret("my-secret-name", max_age=300)

        # Get secret and transform JSON
        secret_json = parameters.get_secret("my-json-secret", transform="json")

        logger.info("Successfully retrieved secrets")

        return {
            'statusCode': 200,
            'body': 'Successfully retrieved secrets'
        }

    except Exception as e:
        logger.error(f"Error retrieving secret: {str(e)}")
        return {
            'statusCode': 500,
            'body': f'Error: {str(e)}'
        }
```

TypeScript

> **Note**
>
> Pour obtenir des exemples complets et des instructions de configuration, consultez la documentation de l'utilitaire de paramètres.

Récupération de secrets depuis Secrets Manager avec l'utilitaire Powertools for AWS Lambda Parameters.

```
import { Logger } from '@aws-lambda-powertools/logger';
import { getSecret } from '@aws-lambda-powertools/parameters/secrets';
import type { Context } from 'aws-lambda';

const logger = new Logger();

export const handler = async (event: any, context: Context) => {
    try {
        // Get secret with caching (default TTL: 5 seconds)
        const secretValue = await getSecret('my-secret-name');

        // Get secret with custom TTL
```

```
        const secretWithTtl = await getSecret('my-secret-name', { maxAge: 300 });

        // Get secret and transform JSON
        const secretJson = await getSecret('my-json-secret', { transform: 'json' });

        logger.info('Successfully retrieved secrets');

        return {
            statusCode: 200,
            body: 'Successfully retrieved secrets'
        };

    } catch (error) {
        logger.error('Error retrieving secret', { error });
        return {
            statusCode: 500,
            body: `Error: ${error}`
        };
    }
};
```

Java

> **Note**
>
> Pour obtenir des exemples complets et des instructions de configuration, consultez la documentation de l'utilitaire de paramètres.

Récupération de secrets depuis Secrets Manager avec l'utilitaire Powertools for AWS Lambda Parameters.

```
import software.amazon.lambda.powertools.logging.Logging;
import software.amazon.lambda.powertools.parameters.SecretsProvider;
import software.amazon.lambda.powertools.parameters.ParamManager;
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;

public class SecretHandler implements RequestHandler<Object, String> {

    private final SecretsProvider secretsProvider =
 ParamManager.getSecretsProvider();
```

```
    @Logging
    @Override
    public String handleRequest(Object input, Context context) {
        try {
            // Get secret with caching (default TTL: 5 seconds)
            String secretValue = secretsProvider.get("my-secret-name");

            // Get secret with custom TTL (300 seconds)
            String secretWithTtl = secretsProvider.withMaxAge(300).get("my-secret-
name");

            // Get secret and transform JSON
            MySecret secretJson = secretsProvider.get("my-json-secret",
 MySecret.class);

            return "Successfully retrieved secrets";

        } catch (Exception e) {
            return "Error retrieving secret: " + e.getMessage();
        }
    }

    public static class MySecret {
        // Define your secret structure here
    }
}
```

.NET

> **Note**
>
> Pour obtenir des exemples complets et des instructions de configuration, consultez la documentation de l'utilitaire de paramètres.

Récupération de secrets depuis Secrets Manager avec l'utilitaire Powertools for AWS Lambda Parameters.

```
using AWS.Lambda.Powertools.Logging;
using AWS.Lambda.Powertools.Parameters;
using Amazon.Lambda.Core;
```

```
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSeriali

public class Function
{
    private readonly ISecretsProvider _secretsProvider;

    public Function()
    {
        _secretsProvider = ParametersManager.SecretsProvider;
    }

    [Logging]
    public async Task<string> FunctionHandler(object input, ILambdaContext context)
    {
        try
        {
            // Get secret with caching (default TTL: 5 seconds)
            var secretValue = await _secretsProvider.GetAsync("my-secret-name");

            // Get secret with custom TTL
            var secretWithTtl = await
 _secretsProvider.WithMaxAge(TimeSpan.FromMinutes(5))
                .GetAsync("my-secret-name");

            // Get secret and transform JSON
            var secretJson = await _secretsProvider.GetAsync<MySecret>("my-json-
secret");

            return "Successfully retrieved secrets";
        }
        catch (Exception e)
        {
            return $"Error retrieving secret: {e.Message}";
        }
    }

    public class MySecret
    {
        // Define your secret structure here
    }
}
```

Configuration et autorisations

Pour utiliser l’utilitaire de paramètres :

1. Installez Powertools AWS Lambda pour votre environnement d'exécution. Pour plus de détails, consultez Outils électriques pour AWS Lambda.
2. Ajoutez les autorisations IAM nécessaires au rôle d’exécution de votre fonction. Pour plus d'informations, consultez Gestion des autorisations dans AWS Lambda.
3. Configurez tous les paramètres facultatifs par le biais de variables d’environnement.

Les autorisations IAM requises sont les mêmes que pour l’approche de l’extension. L'utilitaire gère automatiquement la mise en cache et les appels d'API à Secrets Manager en fonction de votre configuration.

Utilisation de Lambda avec Amazon SQS

> **Note**
>
> Si vous souhaitez envoyer des données à une cible autre qu'une fonction d'événement Lambda ou enrichir les données avant de les envoyer, consultez Amazon EventBridge Pipes.

Vous pouvez utiliser une fonction d'événement Lambda pour traiter les messages d'une file d'attente Amazon Simple Queue Service (Amazon SQS). Lambda prend en charge à la fois les files d'attente standard et les files d'attente FIFO (premier entré, premier sorti) pour les mappages des sources d'événements. Vous pouvez également utiliser le mode provisionné pour allouer des ressources d'interrogation dédiées pour vos mappages de sources d'événements Amazon SQS. La fonction d'événement Lambda et la file d'attente Amazon SQS doivent être Région AWS identiques, bien qu'elles puissent être différentes. Comptes AWS

Pour un exemple de fonction qui traite les messages Amazon SQS, consultez. the section called "didacticiel" Pour le traitement entre comptes, voirthe section called "Tutoriel entre comptes SQS". Pour obtenir la liste complète des options de configuration, consultez the section called "Parameters".

Lorsque vous traitez des messages Amazon SQS, vous devez implémenter une logique de réponse partielle de lot afin d'éviter que les messages traités avec succès soient de nouveau essayés en cas d'échec de certains messages d'un lot. L'utilitaire Batch Processor de Powertools AWS Lambda simplifie cette implémentation en gérant automatiquement la logique de réponse partielle par lots, en réduisant le temps de développement et en améliorant la fiabilité.

Rubriques

- Comprendre le comportement d'interrogation et de traitement par lots pour les mappages des sources d'événements Amazon SQS
- Utilisation du mode provisionné avec les mappages de sources d'événements Amazon SQS
- Configuration du mode provisionné pour le mappage des sources d'événements Amazon SQS
- Exemple d'événement de message de file d'attente standard
- Exemple d'événement de message de file d'attente FIFO
- Création et configuration d'un mappage des sources d'événements Amazon SQS
- Configuration du comportement de mise à l'échelle pour les mappages des sources d'événements SQS

- Gestion des erreurs pour une source d'événements SQS dans Lambda
- Paramètres Lambda pour les mappages des sources d'événement Amazon SQS
- Utilisation du filtrage des événements avec une source d'événement Amazon SQS
- Didacticiel : utilisation de Lambda avec Amazon SQS
- Didacticiel : utilisation d'une file d'attente Amazon SQS entre comptes en tant que source d'événement

Comprendre le comportement d'interrogation et de traitement par lots pour les mappages des sources d'événements Amazon SQS

Avec les mappages des sources d'événements Amazon SQS, Lambda interroge la file d'attente et invoque votre fonction de manière synchrone avec un événement. Chaque événement peut contenir un lot de plusieurs messages provenant de la file d'attente. Lambda reçoit ces événements un lot à la fois, et invoque votre fonction une fois pour chaque lot. Après que la fonction a traité un lot avec succès, Lambda supprime ses messages de la file d'attente.

Quand Lambda reçoit un lot, les messages restent dans la file d'attente mais sont masqués pendant toute la durée du délai de visibilité de la file d'attente. Si votre fonction traite tous les messages d'un lot avec succès, Lambda supprime les messages depuis la file d'attente. Par défaut, si votre fonction rencontre une erreur lors du traitement d'un lot, tous les messages de ce lot redeviennent visibles dans la file d'attente une fois le délai de visibilité expiré. Pour cette raison, le code de votre fonction peut traiter le même message plusieurs fois sans effets secondaires involontaires.

> **Warning**
>
> Les mappages des sources d'événements Lambda traitent chaque événement au moins une fois, et le traitement des enregistrements peut être dupliqué. Pour éviter les problèmes potentiels liés à des événements dupliqués, nous vous recommandons vivement de rendre votre code de fonction idempotent. Pour en savoir plus, consultez Comment rendre ma fonction Lambda idempotente dans le Knowledge Center. AWS

Pour empêcher Lambda de traiter un message plusieurs fois, vous pouvez soit configurer le mappage de votre source d'événements pour inclure les défaillances d'éléments de lot dans la réponse de votre fonction, soit utiliser l'DeleteMessageAPI pour supprimer les messages de la file d'attente au fur et à mesure que votre fonction d'événement Lambda les traite correctement.

Pour de plus amples informations sur les paramètres de configuration pris en charge par Lambda pour les mappages des sources d'événements SQS, consultez the section called "Création d'un mappage des sources d'événements SQS".

Utilisation du mode provisionné avec les mappages de sources d'événements Amazon SQS

Pour les charges de travail où vous devez optimiser le débit de votre mappage des sources d'événements, vous pouvez utiliser le mode provisionné. En mode provisionné, vous définissez des limites minimales et maximales pour le nombre de sondeurs d'événements alloués. Ces sondeurs d'événements alloués sont dédiés à votre mappage des sources d'événements et peuvent gérer les pics de messages inattendus grâce à une mise à l'échelle automatique réactive. Le mappage des sources d'événements Amazon SQS configuré en mode provisionné évolue 3 fois plus vite (jusqu'à 1 000 appels simultanés par minute) et prend en charge une simultanéité 80 fois supérieure (jusqu'à 100 000 appels simultanés) par rapport à la capacité de mappage des sources d'événements Amazon SQS par défaut.

Nous vous recommandons d'utiliser le mode provisionné pour les charges de travail basées sur les événements Amazon SQS soumises à des exigences de performance strictes, telles que les sociétés de services financiers traitant les flux de données du marché, les plateformes de commerce électronique fournissant des recommandations personnalisées en temps réel et les sociétés de jeux gérant les interactions avec les joueurs en direct. L'utilisation du mode alloué génère des coûts supplémentaires. Pour connaître les tarifs détaillés, consultez la section AWS Lambda des prix.

Chaque sondeur d'événements en mode provisionné peut gérer jusqu'à 1 % MB/s du débit, jusqu'à 10 appels simultanés ou jusqu'à 10 appels d'API d'interrogation Amazon SQS par seconde. La plage de valeurs acceptées pour le nombre minimum de sondeurs d'événements (MinimumPollers) est comprise entre 2 et 200, avec une valeur par défaut de 2. La plage de valeurs acceptées pour le nombre maximum de sondeurs d'événements (MaximumPollers) est comprise entre 2 et 10 000, avec une valeur par défaut de 200. MaximumPollers doit être supérieur ou égal à MinimumPollers.

Déterminer les sondeurs d'événements requis

Pour estimer le nombre de sondeurs d'événements nécessaires pour garantir des performances de traitement des messages optimales lors de l'utilisation du mode provisionné pour SQS ESM, collectez les indicateurs suivants pour votre application : pic d'événements SQS par seconde nécessitant un traitement à faible latence, taille moyenne de la charge utile des événements SQS, durée moyenne de la fonction d'événement Lambda et taille de lot configurée.

Vous pouvez d'abord estimer le nombre d'événements SQS par seconde (EPS) pris en charge par un sondeur d'événements pour votre charge de travail à l'aide de la formule suivante :

```
EPS per event poller =
        minimum(
            ceiling(1024 / average event size in KB),
            ceiling(10 / average function duration in seconds) * batch size,
            min(100, 10 * batch size)
                )
```

Ensuite, vous pouvez calculer le nombre minimum de sondeurs requis en utilisant la formule ci-dessous. Ce calcul garantit que vous fournissez une capacité suffisante pour répondre à vos besoins de trafic de pointe.

```
Required event pollers = (Peak number of events per second in Queue) / EPS per event
 poller
```

Prenons l'exemple d'une charge de travail avec une taille de lot par défaut de 10, une taille moyenne des événements de 3 Ko, une durée de fonctionnement moyenne de 100 ms et l'obligation de gérer 1 000 événements par seconde. Dans ce scénario, chaque sondeur d'événements prend en charge environ 100 événements par seconde (EPS). Par conséquent, nous vous recommandons de définir un nombre minimum de sondeurs à 10 afin de répondre de manière adéquate à vos besoins en matière de trafic de pointe. Si votre charge de travail présente les mêmes caractéristiques mais avec une durée de fonctionnement moyenne d'une seconde, chaque sondeur ne prend en charge que 10 EPS, ce qui vous oblige à configurer au moins 100 sondeurs pour prendre en charge 1 000 événements par seconde avec une faible latence.

Nous recommandons d'utiliser une taille de lot par défaut de 10 ou plus pour optimiser l'efficacité des sondeurs d'événements en mode provisionné. Des lots de plus grande taille permettent à chaque sondeur de traiter un plus grand nombre d'événements par appel, ce qui améliore le débit et la rentabilité. Lorsque vous planifiez votre capacité de sondeurs d'événements, tenez compte des pics de trafic potentiels et envisagez de définir une valeur de minimumPollers légèrement supérieure au minimum calculé pour créer une zone tampon. En outre, surveillez les caractéristiques de votre charge de travail au fil du temps, car les modifications de la taille des messages, de la durée des fonctions ou des modèles de trafic peuvent nécessiter des ajustements de la configuration de votre sondeur d'événements afin de maintenir des performances et une rentabilité optimales. Pour une planification précise de la capacité, nous vous recommandons de tester votre charge de travail spécifique afin de déterminer l'EPS réel que chaque enquêteur peut piloter.

Configuration du mode provisionné pour le mappage des sources d'événements Amazon SQS

Vous pouvez configurer le mode provisionné pour le mappage de vos sources d'événements Amazon SQS à l'aide de la console ou de l'API Lambda.

Pour configurer le mode provisionné pour un mappage de source d'événements Amazon SQS existant (console)

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez la fonction avec le mappage des sources d'événements Amazon SQS pour laquelle vous souhaitez configurer le mode provisionné.
3. Choisissez Configuration, puis Déclencheurs.
4. Choisissez le mappage des sources d'événements Amazon SQS pour lequel vous souhaitez configurer le mode provisionné, puis choisissez Modifier.
5. Sous Configuration du mappage des sources d’événements, choisissez Configurer le mode provisionné.
   - Pour le nombre minimal de sondeurs, entrez une valeur comprise entre 2 et 200. Si vous ne spécifiez aucune valeur, Lambda choisit une valeur par défaut de 2.
   - Pour le nombre maximal de sondeurs d'événements, entrez une valeur comprise entre 2 et 10 000. Cette valeur doit être supérieure ou égale à la valeur du Nombre minimal de sondeurs d’événements. Si vous ne spécifiez aucune valeur, Lambda choisit la valeur par défaut 200.
6. Cliquez sur Enregistrer.

Vous pouvez configurer le mode provisionné par programmation à l'aide de l'`ProvisionedPollerConfig`objet de votre. `EventSourceMappingConfiguration` Par exemple, la commande `UpdateEventSourceMapping` CLI suivante configure une `MinimumPollers` valeur de 5 et une `MaximumPollers` valeur de 100.

```
aws lambda update-event-source-mapping \
    --uuid a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
    --provisioned-poller-config '{"MinimumPollers": 5, "MaximumPollers": 100}'
```

Après avoir configuré le mode alloué, vous pouvez observer l’utilisation des sondeurs d’événements pour votre charge de travail en surveillant la métrique `ProvisionedPollers`. Pour plus d'informations, consultez la section Métriques de mappage des sources d'événements.

Pour désactiver le mode provisionné et revenir au mode par défaut (à la demande), vous pouvez utiliser la commande `UpdateEventSourceMapping` CLI suivante :

```
aws lambda update-event-source-mapping \
    --uuid a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
    --provisioned-poller-config '{}'
```

> **Note**
>
> Le mode provisionné ne peut pas être utilisé conjointement avec le paramètre de simultanéité maximale. Lorsque vous utilisez le mode provisionné, vous contrôlez la simultanéité maximale grâce au nombre maximal de sondeurs d'événements.

Pour plus d'informations sur la configuration du mode provisionné, consultezthe section called “Création d’un mappage”.

Exemple d’événement de message de file d’attente standard

ExampleÉvénement de message Amazon SQS (file d’attente standard)

```
{
    "Records": [
        {
            "messageId": "059f36b4-87a3-44ab-83d2-661975830a7d",
            "receiptHandle": "AQEBwJnKyrHigUMZj6rYigCgxlaS3SLy0a...",
            "body": "Test message.",
            "attributes": {
                "ApproximateReceiveCount": "1",
                "SentTimestamp": "1545082649183",
                "SenderId": "AIDAIENQZJOLO23YVJ4VO",
                "ApproximateFirstReceiveTimestamp": "1545082649185"
            },
            "messageAttributes": {
                "myAttribute": {
                    "stringValue": "myValue",
                    "stringListValues": [],
                    "binaryListValues": [],
                    "dataType": "String"
                }
            },
```

```
            "md5OfBody": "e4e68fb7bd0e697a0ae8f1bb342846b3",
            "eventSource": "aws:sqs",
            "eventSourceARN": "arn:aws:sqs:us-east-2:123456789012:my-queue",
            "awsRegion": "us-east-2"
        },
        {
            "messageId": "2e1424d4-f796-459a-8184-9c92662be6da",
            "receiptHandle": "AQEBzWwaftRI0KuVm4tP+/7q1rGgNqicHq...",
            "body": "Test message.",
            "attributes": {
                "ApproximateReceiveCount": "1",
                "SentTimestamp": "1545082650636",
                "SenderId": "AIDAIENQZJOLO23YVJ4VO",
                "ApproximateFirstReceiveTimestamp": "1545082650649"
            },
            "messageAttributes": {},
            "md5OfBody": "e4e68fb7bd0e697a0ae8f1bb342846b3",
            "eventSource": "aws:sqs",
            "eventSourceARN": "arn:aws:sqs:us-east-2:123456789012:my-queue",
            "awsRegion": "us-east-2"
        }
    ]
}
```

Par défaut, Lambda interroge jusqu'à 10 messages à la fois dans votre file d'attente, et envoie ce lot à votre fonction. Pour éviter d'invoquer la fonction avec un petit nombre d'enregistrements, vous pouvez configurer la source d'événement de manière à les mettre en mémoire tampon pendant 5 minutes en configurant une fenêtre de lot. Avant d'invoquer la fonction, Lambda continue d'interroger les messages de la file d'attente standard jusqu'à ce que la fenêtre de lot expire, que le quota de taille des données utiles de l'invocation soit atteint ou que la taille maximale configurée du lot soit atteinte.

Si vous utilisez une fenêtre de lot et que votre file d'attente SQS contient un trafic très faible, Lambda peut attendre 20 secondes avant d'invoquer votre fonction. C'est le cas même si vous définissez une fenêtre de lot inférieure à 20 secondes.

> **Note**
>
> Sous Java, vous pouvez rencontrer des erreurs de pointeur nul lors de la désérialisation de JSON. Cela peut être dû à la façon dont les cas « Records » (Enregistrements) et « eventSourceARN » sont convertis par le mappeur d'objets JSON.

Exemple d'événement de message de file d'attente FIFO

Pour les files d'attente FIFO, les enregistrements contiennent des attributs supplémentaires liés à la déduplication et au séquençage.

ExampleÉvénement de message Amazon SQS (file d'attente FIFO)

```
{
    "Records": [
        {
            "messageId": "11d6ee51-4cc7-4302-9e22-7cd8afdaadf5",
            "receiptHandle": "AQEBBX8nesZEXmkhsmZeyIE8iQAMig7qw...",
            "body": "Test message.",
            "attributes": {
                "ApproximateReceiveCount": "1",
                "SentTimestamp": "1573251510774",
                "SequenceNumber": "18849496460467696128",
                "MessageGroupId": "1",
                "SenderId": "AIDAIO23YVJENQZJOL4VO",
                "MessageDeduplicationId": "1",
                "ApproximateFirstReceiveTimestamp": "1573251510774"
            },
            "messageAttributes": {},
            "md5OfBody": "e4e68fb7bd0e697a0ae8f1bb342846b3",
            "eventSource": "aws:sqs",
            "eventSourceARN": "arn:aws:sqs:us-east-2:123456789012:fifo.fifo",
            "awsRegion": "us-east-2"
        }
    ]
}
```

Création et configuration d'un mappage des sources d'événements Amazon SQS

Pour traiter les messages Amazon SQS avec Lambda, configurez votre file d'attente avec les paramètres appropriés, puis créez un mappage des sources d'événements Lambda.

Rubriques

- Configuration d'une file d'attente à utiliser avec Lambda
- Configuration des autorisations de rôle d'exécution Lambda
- Création d'un mappage des sources d'événements SQS

Configuration d'une file d'attente à utiliser avec Lambda

Si vous ne possédez pas encore de file d'attente Amazon SQS, créez-en une qui servira de source d'événements pour votre fonction d'événement Lambda. La fonction d'événement Lambda et la file d'attente Amazon SQS doivent être Région AWS identiques, bien qu'elles puissent être différentes. Comptes AWS

Pour laisser à votre fonction le temps de traiter chaque lot d'enregistrements, définissez le délai de visibilité de la file d'attente source à au moins six fois le délai de configuration sur votre fonction. Le délai supplémentaire permet à Lambda d'effectuer une nouvelle tentative si l'exécution de la fonction est limitée pendant le traitement d'un lot précédent.

> **Note**
>
> Le délai d'expiration de votre fonction doit être inférieur ou égal au délai d'expiration de visibilité de la file d'attente. Lambda valide cette exigence lorsque vous créez ou mettez à jour un mappage de source d'événements et renvoie une erreur si le délai d'expiration de la fonction dépasse le délai de visibilité de la file d'attente.

Par défaut, si Lambda rencontre une erreur à un moment donné lors du traitement d'un lot, tous les messages de ce lot retournent dans la file d'attente. Après le délai de visibilité, les messages redeviennent visibles pour Lambda. Vous pouvez configurer le mappage des sources d'événements pour utiliser les réponses par lots partielles afin que seuls les messages ayant échoué soient renvoyés dans la file d'attente.

En outre, en cas d'échec répété du traitement d'un message, Amazon SQS peut envoyer celui-ci à une file d'attente de lettres mortes. Nous vous recommandons de définir `maxReceiveCount` sur la stratégie de redirection de votre file d'attente source sur au moins 5. Cela donne à Lambda la possibilité d'effectuer quelques tentatives avant d'envoyer les messages ayant échoué directement à la file d'attente de lettres mortes.

Configuration des autorisations de rôle d'exécution Lambda

La politique AWSLambdaSQSQueueExecutionRole AWS gérée inclut les autorisations dont Lambda a besoin pour lire depuis votre file d'attente Amazon SQS. Vous pouvez ajouter cette politique gérée au rôle d'exécution de votre fonction.

En option, si vous utilisez une file d'attente chiffrée, vous devez également ajouter l'autorisation suivante à votre rôle d'exécution :

- kms:Decrypt

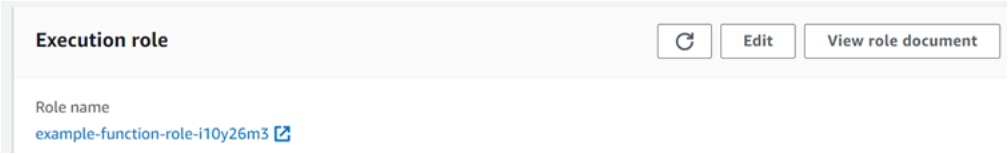
Création d'un mappage des sources d'événements SQS

Créez un mappage de source d'événements pour indiquer à Lambda d'envoyer des éléments de votre file d'attente vers une fonction d'événement Lambda. Vous pouvez créer plusieurs mappages de source d'événement pour traiter des éléments de plusieurs files d'attente avec une seule fonction. Quand Lambda invoque la fonction cible, l'événement peut contenir plusieurs éléments, jusqu'à une taille de lot maximale configurable.

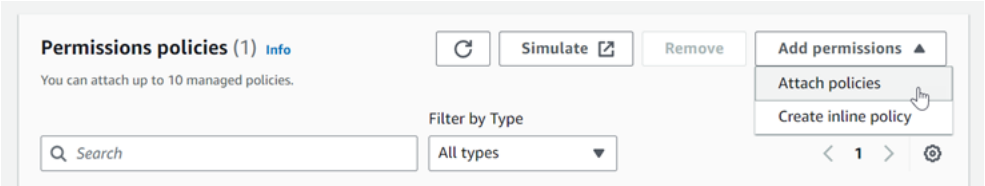
Pour configurer votre fonction afin qu'elle puisse lire depuis Amazon SQS, associez la politique AWSLambdaSQSQueueExecutionRole AWS gérée à votre rôle d'exécution. Créez ensuite un mappage des sources d'événements SQS à partir de la console en suivant les étapes suivantes.

Pour ajouter des autorisations et créer un déclencheur

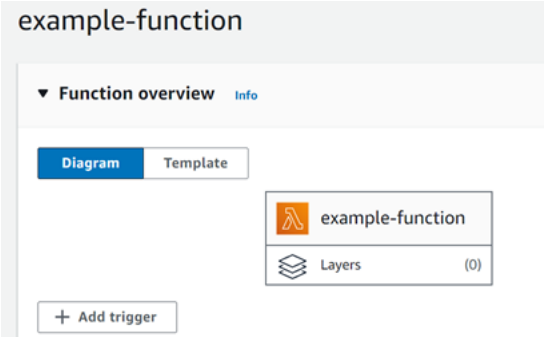
1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez le nom d'une fonction.
3. Choisissez l'onglet Configuration, puis Permissions (Autorisations).
4. Sous Nom du rôle, cliquez sur le lien vers votre rôle d'exécution. Ce lien ouvre le rôle dans la console IAM.



5. Choisissez Ajouter des autorisations, puis Attacher des politiques.



6. Dans le champ de recherche, entrez `AWSLambdaSQSQueueExecutionRole`. Ajoutez cette politique à votre rôle d'exécution. Il s'agit d'une politique AWS gérée qui contient les autorisations dont votre fonction a besoin pour lire depuis une file d'attente Amazon SQS. Pour plus d'informations sur cette politique, consultez AWSLambdaSQSQueueExecutionRolela référence des politiques AWS gérées.
7. Revenez à votre fonction dans la console Lambda. Sous Function overview (Vue d'ensemble de la fonction), choisissez Add trigger (Ajouter un déclencheur).



8. Choisissez un type de déclencheur.
9. Configurez les options requises, puis choisissez Add (Ajouter).

Lambda prend en charge les options de configuration suivantes pour les sources d'événements Amazon SQS :

File d'attente SQS

La file d'attente Amazon SQS à partir de laquelle lire les enregistrements. La fonction d'événement Lambda et la file d'attente Amazon SQS doivent être Région AWS identiques, bien qu'elles puissent être différentes. Comptes AWS

Activation du déclencheur

L'état du mappage des sources d'événements. Activez le déclencheur est sélectionné par défaut.

Taille de lot

Le nombre maximum d'enregistrements à envoyer à la fonction dans chaque lot. Pour une file d'attente standard, cela peut aller jusqu'à 10 000 registres. Pour une file d'attente FIFO, le maximum est de 10. Pour une taille de lot supérieure à 10, vous devez également définir la fenêtre de lot (`MaximumBatchingWindowInSeconds`) sur au moins 1 seconde.

Configurez le délai d'attente de votre fonction de façon à laisser suffisamment de temps pour traiter le lot entier d'éléments. Si les éléments sont longs à traiter, choisissez une taille de lot plus petite. Une grande taille de lot peut améliorer l'efficacité pour des charges de travail qui sont très rapides ou qui induisent beaucoup d'efforts supplémentaires. Si vous configurez une simultanéité réservée sur votre fonction, définissez un minimum de cinq exécutions simultanées pour réduire le risque d'erreurs de limitation lorsque Lambda invoque votre fonction.

Lambda transmet tous les registres du lot à la fonction en un seul appel, tant que la taille totale des événements ne dépasse pas le quota de taille des données utiles d'invocation pour une

invocation synchrone (6 Mo). Des métadonnées sont générées par Lambda et Amazon SQS pour chaque registre. Ces métadonnées supplémentaires sont comptabilisées dans la taille de charge utile totale, ce qui peut entraîner l'envoi dans un lot d'un nombre total d'enregistrements inférieur à la taille du lot configuré. Les champs de métadonnées qu'Amazon SQS envoie peuvent être de longueur variable. Pour plus d'informations sur les champs de métadonnées Amazon SQS, consultez la documentation relative aux opérations d'ReceiveMessageAPI dans le manuel Amazon Simple Queue Service API Reference.

Fenêtre de lot

Intervalle de temps maximal (en secondes) pour collecter des enregistrements avant d'invoquer la fonction. Cela s'applique uniquement aux files d'attente standards.

Si vous utilisez une fenêtre de lot supérieure à 0 seconde, vous devez tenir compte de l'augmentation du temps de traitement dans le délai de visibilité de votre file d'attente. Nous vous recommandons de définir le délai de visibilité de votre file d'attente à six fois le délai d'expiration de la fonction d'événement, plus la valeur de. `MaximumBatchingWindowInSeconds` Cela laisse le temps à votre fonction d'événement Lambda de traiter chaque lot d'événements et de réessayer en cas d'erreur de régulation.

Lorsque les messages sont disponibles, Lambda commence à les traiter par lots. Lambda commence à traiter cinq lots à la fois avec cinq invocations simultanés de votre fonction. Si les messages sont toujours disponibles, Lambda ajoute jusqu'à 300 appels simultanés de votre fonction par minute, jusqu'à un maximum de 1 250 appels simultanés.

En mode provisionné, chaque sondeur d'événements peut gérer jusqu'à 1 % MB/s du débit, jusqu'à 10 appels simultanés ou jusqu'à 10 appels d'API d'interrogation Amazon SQS par seconde. Lambda adapte le nombre de sondeurs d'événements entre le minimum et le maximum configurés, en ajoutant rapidement jusqu'à 1 000 appels simultanés par minute afin de fournir un traitement à faible latence de vos événements Amazon SQS. Vous pouvez contrôler la mise à l'échelle et la simultanéité grâce à ces paramètres minimaux et maximaux d'un sondeur d'événements. Pour en savoir plus sur la mise à l'échelle et la simultanéité des fonctions d'événement, consultezComprendre le dimensionnement des fonctions d'événement Lambda.

Pour traiter davantage de messages, vous pouvez optimiser votre fonction d'événement Lambda pour un débit plus élevé. Pour plus d'informations, consultez Comprendre comment s' AWS Lambda adapte aux files d'attente standard Amazon SQS.

Critères de filtrage

Ajoutez des critères de filtrage pour contrôler les événements que Lambda envoie à votre fonction pour traitement. Pour plus d'informations, consultez Contrôlez les événements que Lambda envoie à votre fonction d'événement.

Simultanéité maximum

Le nombre maximum de fonctions simultanées que la source d'événement peut invoquer. Ne peut pas être utilisé lorsque le mode provisionné est activé. Pour plus d'informations, consultez Configuration de la simultanéité maximale pour les sources d'événements Amazon SQS.

Mode alloué

Lorsque cette option est activée, alloue des ressources de sondage dédiées au mappage des sources de votre événement. Vous pouvez configurer le nombre minimum (2-200) et maximum (2-2000) de sondeurs d'événements. Chaque sondeur d'événements peut gérer jusqu'à 1 % MB/sec du débit, jusqu'à 10 appels simultanés ou jusqu'à 10 appels d'API d'interrogation Amazon SQS par seconde.

> **Note**
>
> Remarque : vous ne pouvez pas utiliser simultanément le mode provisionné et la simultanéité maximale. Lorsque le mode provisionné est activé, utilisez le paramètre du nombre maximum de sondeurs pour contrôler la simultanéité.

Configuration du comportement de mise à l'échelle pour les mappages des sources d'événements SQS

Vous pouvez contrôler le comportement de dimensionnement de vos mappages de sources d'événements Amazon SQS via des paramètres de simultanéité maximale ou en activant le mode provisionné. Ces options s'excluent mutuellement.

Par défaut, Lambda met à l'échelle automatiquement les observateurs d'événements en fonction du volume des messages. Lorsque vous activez le mode provisionné, vous allouez un nombre minimum et maximum de ressources de sondage dédiées qui restent prêtes à gérer les modèles de trafic attendus. Vous pouvez optimiser les performances de votre mappage des sources d'événements de deux manières :

- Mode standard (par défaut) : Lambda gère automatiquement le dimensionnement, en commençant par un petit nombre de sondeurs, puis en augmentant ou en diminuant en fonction de la charge de travail.
- Mode provisionné : vous configurez des ressources d'interrogation dédiées avec des limites minimales et maximales, ce qui permet une mise à l'échelle 3 fois plus rapide et une capacité de traitement jusqu'à 16 fois supérieure.

Pour les files d’attente standard, Lambda utilise une interrogation longue pour interroger une file d’attente jusqu’à ce qu’elle devienne active. Lorsque les messages sont disponibles, Lambda commence à traiter cinq lots à la fois avec cinq appels simultanés de votre fonction d'événement. Si les messages sont toujours disponibles, Lambda augmente le nombre de processus lisant des lots de 300 appels simultanés supplémentaires par minute. Le nombre maximum d'appels qu'un mappage de source d'événement peut traiter simultanément est de 1 250. Lorsque le trafic est faible, Lambda réduit le traitement à cinq appels simultanés et peut l'optimiser jusqu'à deux appels simultanés afin de réduire les appels Amazon SQS et les coûts correspondants. Toutefois, cette optimisation n’est pas disponible lorsque vous activez le paramètre de simultanéité maximale.

Pour les files d’attente FIFO, Lambda envoie les messages à votre fonction dans l’ordre de leur réception. Lorsque vous envoyez un message à une file d’attente FIFO, vous spécifiez un ID de groupe de messages. Amazon SQS veille à ce que les messages du même groupe soient livrés à Lambda dans l’ordre. Lorsque Lambda lit vos messages par lots, chaque lot peut contenir des messages provenant de plusieurs groupes de messages, mais l'ordre des messages est conservé. Si la fonction renvoie une erreur, toutes les nouvelles tentatives sont effectuées sur les messages concernés avant que Lambda reçoive des messages supplémentaires du même groupe.

En mode provisionné, chaque sondeur d'événements peut gérer jusqu'à 1 % MB/sec du débit, jusqu'à 10 appels simultanés ou jusqu'à 10 appels d'API d'interrogation Amazon SQS par seconde. Lambda adapte le nombre d'interrogateurs d'événements entre le minimum et le maximum configurés, en ajoutant rapidement jusqu'à 1 000 appels simultanés par minute afin de fournir un traitement cohérent et à faible latence de vos événements Amazon SQS. L’utilisation du mode alloué génère des coûts supplémentaires. Pour connaître les tarifs détaillés, consultez la section AWS Lambda des prix.

Chaque sondeur d'événements utilise de longs sondages dans votre file d'attente SQS, avec jusqu'à 10 sondages par seconde, ce qui entraîne des coûts liés aux demandes d'API SQS. Consultez la tarification d'Amazon SQS pour plus de détails. Vous pouvez contrôler la mise à l'échelle et la simultanéité par le biais de ces paramètres minimaux et maximaux d'un sondeur d'événements, plutôt

que d'utiliser le paramètre de simultanéité maximale, car ces options ne peuvent pas être utilisées conjointement.

> **Note**
>
> Vous ne pouvez pas utiliser le paramètre de simultanéité maximale et le mode provisionné en même temps. Lorsque le mode provisionné est activé, vous contrôlez le dimensionnement et la simultanéité du mappage de votre source d'événements Amazon SQS via le nombre minimum et maximum de sondeurs d'événements.

Configuration de la simultanéité maximale pour les sources d’événements Amazon SQS

Vous pouvez utiliser le paramètre de simultanéité maximale pour contrôler le comportement de mise à l’échelle de vos sources d’événements SQS. Notez que la simultanéité maximale ne peut pas être utilisée lorsque le mode provisionné est activé. Le paramètre de simultanéité maximale limite le nombre d’instances simultanées de la fonction qu’une source d’événements Amazon SQS peut invoquer. La simultanéité maximale est un paramètre de niveau source d’événement. Si vous avez plusieurs sources d’événements Amazon SQS mappées à une fonction, chaque source d’événements peut avoir un paramètre de simultanéité maximale séparé.

Vous pouvez utiliser la simultanéité maximale pour empêcher une file d’attente d’utiliser toute la simultanéité réservée de la fonction ou le reste du quota de simultanéité du compte. La configuration de la simultanéité maximale sur une source d’événements Amazon SQS est gratuite.

Il est important de noter que la simultanéité maximale et la simultanéité réservée sont deux paramètres indépendants. Ne définissez pas une simultanéité maximale supérieure à la simultanéité réservée de la fonction. Si vous configurez la simultanéité maximale, assurez-vous que la simultanéité réservée de votre fonction est supérieure ou égale à la simultanéité maximale totale pour toutes les sources d’événements Amazon SQS sur la fonction. Sinon, Lambda pourrait limiter vos messages.

Lorsque le quota de simultanéité de votre compte est défini sur la valeur par défaut de 1 000, un mappage des sources d’événements Amazon SQS peut être mis à l’échelle pour invoquer des instances de fonction jusqu’à cette valeur, sauf si vous spécifiez une simultanéité maximale.

Si vous recevez une augmentation du quota de simultanéité par défaut de votre compte, Lambda risque de ne pas être en mesure d'invoquer des instances de fonctions concurrentes jusqu'à votre nouveau quota. Par défaut, Lambda peut effectuer une mise à l’échelle pour invoquer

jusqu'à 1 250 instances de fonctions simultanées pour un mappage des sources d'événements Amazon SQS. Si vous avez besoin d'une plus grande simultanéité, activez le mode provisionné. Le mode provisionné permet d'effectuer jusqu'à 100 000 appels de fonctions simultanés. Pour plus d'informations, consultez Utilisation du mode provisionné avec les mappages de sources d'événements Amazon SQS.

> **Note**
>
> Pour les files d'attente FIFO, les invocations simultanées sont limitées soit par le nombre d'ID de groupes de messages (`messageGroupId`), soit par le paramètre de simultanéité maximal, selon ce qui est le plus bas. Par exemple, si vous avez six ID de groupe de messages et que la simultanéité maximale est fixée à dix, votre fonction peut avoir un maximum de six invocations simultanées.

Vous pouvez configurer la simultanéité maximale sur les mappages des sources d'événements Amazon SQS nouveaux et existants.

Configuration de la simultanéité maximale à l'aide de la console Lambda

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez le nom d'une fonction.
3. Sous Function overview (Vue d'ensemble des fonctions), choisissez SQS. Cela ouvre l'onglet Configuration.
4. Sélectionnez le déclencheur Amazon SQS et choisissez Edit (Modifier).
5. Pour Maximum concurrency (Simultanéité maximale), saisissez un nombre compris entre 2 et 1 000. Pour désactiver la simultanéité maximale, laissez la case vide.
6. Cliquez sur Enregistrer.

Configurez la simultanéité maximale à l'aide du AWS Command Line Interface (AWS CLI)

Utilisez la commande update-event-source-mapping avec l'option `--scaling-config`. Exemple :

```
aws lambda update-event-source-mapping \
    --uuid "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE" \
    --scaling-config '{"MaximumConcurrency":5}'
```

Pour désactiver la simultanéité maximale, entrez une valeur vide pour `--scaling-config` :

```
aws lambda update-event-source-mapping \
    --uuid "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE" \
    --scaling-config "{}"
```

Configuration de la simultanéité maximale à l'aide de l'API Lambda

Utilisez l'UpdateEventSourceMappingaction CreateEventSourceMappingou avec un ScalingConfigobjet.

Gestion des erreurs pour une source d'événements SQS dans Lambda

Pour gérer les erreurs liées à une source d'événement SQS, Lambda utilise automatiquement une stratégie de nouvelle tentative associée à une stratégie de backoff. Vous pouvez également personnaliser le comportement de gestion des erreurs en configurant votre mappage des sources d'événements SQS de manière à renvoyer des réponses par lots partielles.

Stratégie d'interruption pour les invocations ayant échoué

Lorsqu'une invocation échoue, Lambda tente de réessayer l'invocation tout en mettant en œuvre une stratégie d'interruption. La stratégie d'interruption diffère légèrement selon que Lambda a rencontré l'échec à cause d'une erreur dans votre code de fonction, ou à cause de la limitation.

- Si le code de votre fonction d'événement est à l'origine de l'erreur, Lambda arrête le traitement et tente à nouveau l'appel. Dans le même temps, Lambda réduit progressivement les tentatives en diminuant la quantité de simultanéité allouée à votre mappage des sources d'événements Amazon SQS. Lorsque le délai de visibilité de votre file d'attente est expiré, le message réapparaît dans la file d'attente.
- Si l'invocation échoue en raison d'une limitation, Lambda réduit progressivement les tentatives en diminuant la quantité de simultanéité allouée à votre mappage des sources d'événements Amazon SQS. Lambda continue à réessayer le message jusqu'à ce que l'horodatage du message dépasse le délai de visibilité de votre file d'attente, auquel cas Lambda abandonne le message.

Mise en œuvre de réponses partielles de lot

Lorsque votre fonction d'événement Lambda rencontre une erreur lors du traitement d'un lot, tous les messages de ce lot sont à nouveau visibles dans la file d'attente par défaut, y compris les messages

que Lambda a traités avec succès. Par conséquent, votre fonction peut finir par traiter le même message plusieurs fois.

Pour éviter de retraiter les messages traités avec succès d'un lot en échec, vous pouvez configurer le mappage des sources d'événements pour que seuls les messages ayant échoué soient à nouveau visibles. C'est ce que l'on appelle une réponse partielle de lot. Pour activer les réponses partielles par lots, spécifiez `ReportBatchItemFailures` l'FunctionResponseTypesaction lors de la configuration du mappage des sources d'événements. Avec ce paramètre, votre fonction peut renvoyer un résultat partiel, ce qui peut contribuer à réduire le nombre de tentatives inutiles sur les enregistrements.

> **Note**
>
> L'utilitaire Batch Processor de Powertools for AWS Lambda gère automatiquement toute la logique de réponse partielle par lots. Cet utilitaire simplifie la mise en œuvre de modèles de traitement par lots et réduit le code personnalisé nécessaire pour gérer correctement les échecs d'éléments de lots. Il est disponible pour Python, Java, TypeScript et .NET.

Lorsque `ReportBatchItemFailures` est activé, Lambda ne réduit pas la taille de l'interrogation des messages lorsque les invocations de fonctions échouent. Si vous vous attendez à ce que certains messages échouent et que vous ne voulez pas que ces échecs aient un impact sur le taux de traitement des messages, utilisez `ReportBatchItemFailures`.

> **Note**
>
> Gardez les points suivants à l'esprit lorsque vous utilisez des réponses partielles de lot :
>
> - Si la fonction génère une exception, l'ensemble du lot est considéré comme un échec complet.
> - Si vous utilisez cette fonctionnalité avec une file d'attente FIFO, votre fonction doit arrêter le traitement des messages après le premier échec et renvoyer tous les messages échoués et non traités dans `batchItemFailures`. Cela permet de préserver l'ordre des messages dans votre file d'attente.

Pour activer les rapports partiels de lot

1. Consultez les bonnes pratiques pour la mise en œuvre des réponses partielles de lot.

2. Exécutez la commande suivante pour activer `ReportBatchItemFailures` pour votre fonction. Pour récupérer l'UUID du mappage de votre source d'événements, exécutez la commande AWS CLI list-event-source-mappings.

```
aws lambda update-event-source-mapping \
--uuid "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE" \
--function-response-types "ReportBatchItemFailures"
```

3. Mettez à jour le code de votre fonction afin de capturer toutes les exceptions et de renvoyer les messages d'échec dans une réponse JSON `batchItemFailures`. La réponse `batchItemFailures` doit inclure une liste d'identifiants de message, sous forme de valeurs JSON `itemIdentifier`.

   Supposons par exemple que vous avez un lot de cinq messages avec des identifiants de message `id1`, `id2`, `id3`, `id4` et `id5`. Votre fonction traite avec succès `id1`, `id3` et `id5`. Pour rendre les messages `id2` et `id4` visibles de nouveau dans la file d'attente, votre fonction doit renvoyer la réponse suivante :

```
{
  "batchItemFailures": [
        {
            "itemIdentifier": "id2"
        },
        {
            "itemIdentifier": "id4"
        }
    ]
}
```

   Voici quelques exemples de codes de fonctions qui renvoient la liste des identifiants des messages ayant échoué dans le lot :

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signalement des échecs d'articles par lots SQS avec Lambda à l'aide de .NET.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
using Amazon.Lambda.Core;
using Amazon.Lambda.SQSEvents;

// Assembly attribute to enable the Lambda function's JSON input to be
 converted into a .NET class.
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJson
namespace sqsSample;

public class Function
{
    public async Task<SQSBatchResponse> FunctionHandler(SQSEvent evnt,
 ILambdaContext context)
    {
        List<SQSBatchResponse.BatchItemFailure> batchItemFailures = new
 List<SQSBatchResponse.BatchItemFailure>();
        foreach(var message in evnt.Records)
        {
            try
            {
                //process your message
                await ProcessMessageAsync(message, context);
            }
            catch (System.Exception)
            {
                //Add failed message identifier to the batchItemFailures list
```

```
                batchItemFailures.Add(new
 SQSBatchResponse.BatchItemFailure{ItemIdentifier=message.MessageId});
            }
        }
        return new SQSBatchResponse(batchItemFailures);
    }

    private async Task ProcessMessageAsync(SQSEvent.SQSMessage message,
 ILambdaContext context)
    {
        if (String.IsNullOrEmpty(message.Body))
        {
            throw new Exception("No Body in SQS Message.");
        }
        context.Logger.LogInformation($"Processed message {message.Body}");
        // TODO: Do interesting work based on the new message
        await Task.CompletedTask;
    }
}
```

Go

Kit SDK pour Go V2

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signalement des échecs d'articles par lots SQS avec Lambda à l'aide de Go.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package main

import (
 "context"
 "fmt"
 "github.com/aws/aws-lambda-go/events"
 "github.com/aws/aws-lambda-go/lambda"
```

```
)

func handler(ctx context.Context, sqsEvent events.SQSEvent)
 (map[string]interface{}, error) {
 batchItemFailures := []map[string]interface{}{}

 for _, message := range sqsEvent.Records {
  if len(message.Body) > 0 {
   // Your message processing condition here
   fmt.Printf("Successfully processed message: %s\n", message.Body)
  } else {
   // Message processing failed
   fmt.Printf("Failed to process message %s\n", message.MessageId)
   batchItemFailures = append(batchItemFailures, map[string]interface{}
{"itemIdentifier": message.MessageId})
  }
 }

 sqsBatchResponse := map[string]interface{}{
  "batchItemFailures": batchItemFailures,
 }
 return sqsBatchResponse, nil
}

func main() {
 lambda.Start(handler)
}
```

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signalement des échecs d'articles par lots SQS avec Lambda à l'aide de Java.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.SQSEvent;
import com.amazonaws.services.lambda.runtime.events.SQSBatchResponse;

import java.util.ArrayList;
import java.util.List;

public class ProcessSQSMessageBatch implements RequestHandler<SQSEvent,
 SQSBatchResponse> {
    @Override
    public SQSBatchResponse handleRequest(SQSEvent sqsEvent, Context context)
 {
        List<SQSBatchResponse.BatchItemFailure> batchItemFailures = new
 ArrayList<SQSBatchResponse.BatchItemFailure>();

        for (SQSEvent.SQSMessage message : sqsEvent.getRecords()) {
            try {
                //process your message
            } catch (Exception e) {
                //Add failed message identifier to the batchItemFailures
 list
                batchItemFailures.add(new
 SQSBatchResponse.BatchItemFailure(message.getMessageId()));
            }
        }
        return new SQSBatchResponse(batchItemFailures);
    }
}
```

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signaler les défaillances d'éléments de lot SQS avec JavaScript Lambda à l'aide de.

```
// Node.js 20.x Lambda runtime, AWS SDK for Javascript V3
export const handler = async (event, context) => {
    const batchItemFailures = [];
    for (const record of event.Records) {
        try {
            await processMessageAsync(record, context);
        } catch (error) {
            batchItemFailures.push({ itemIdentifier: record.messageId });
        }
    }
    return { batchItemFailures };
};

async function processMessageAsync(record, context) {
    if (record.body && record.body.includes("error")) {
        throw new Error("There is an error in the SQS Message.");
    }
    console.log(`Processed message: ${record.body}`);
}
```

Signaler les défaillances d'éléments de lot SQS avec TypeScript Lambda à l'aide de.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import { SQSEvent, SQSBatchResponse, Context, SQSBatchItemFailure,
 SQSRecord } from 'aws-lambda';

export const handler = async (event: SQSEvent, context: Context):
 Promise<SQSBatchResponse> => {
    const batchItemFailures: SQSBatchItemFailure[] = [];

    for (const record of event.Records) {
        try {
            await processMessageAsync(record);
        } catch (error) {
            batchItemFailures.push({ itemIdentifier: record.messageId });
        }
    }
```

```
    return {batchItemFailures: batchItemFailures};
};

async function processMessageAsync(record: SQSRecord): Promise<void> {
    if (record.body && record.body.includes("error")) {
        throw new Error('There is an error in the SQS Message.');
    }
    console.log(`Processed message ${record.body}`);
}
```

PHP

Kit SDK pour PHP

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signalement des échecs d'articles par lots SQS avec Lambda à l'aide de PHP.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
<?php

use Bref\Context\Context;
use Bref\Event\Sqs\SqsEvent;
use Bref\Event\Sqs\SqsHandler;
use Bref\Logger\StderrLogger;

require __DIR__ . '/vendor/autoload.php';

class Handler extends SqsHandler
{
    private StderrLogger $logger;
    public function __construct(StderrLogger $logger)
    {
        $this->logger = $logger;
    }
```

```
    /**
     * @throws JsonException
     * @throws \Bref\Event\InvalidLambdaEvent
     */
    public function handleSqs(SqsEvent $event, Context $context): void
    {
        $this->logger->info("Processing SQS records");
        $records = $event->getRecords();

        foreach ($records as $record) {
            try {
                // Assuming the SQS message is in JSON format
                $message = json_decode($record->getBody(), true);
                $this->logger->info(json_encode($message));
                // TODO: Implement your custom processing logic here
            } catch (Exception $e) {
                $this->logger->error($e->getMessage());
                // failed processing the record
                $this->markAsFailed($record);
            }
        }
        $totalRecords = count($records);
        $this->logger->info("Successfully processed $totalRecords SQS
 records");
    }
}

$logger = new StderrLogger();
return new Handler($logger);
```

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signalement des échecs d'articles par lots SQS avec Lambda à l'aide de Python.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0

def lambda_handler(event, context):
    if event:
        batch_item_failures = []
        sqs_batch_response = {}

        for record in event["Records"]:
            try:
                print(f"Processed message: {record['body']}")
            except Exception as e:
                batch_item_failures.append({"itemIdentifier":
 record['messageId']})

        sqs_batch_response["batchItemFailures"] = batch_item_failures
        return sqs_batch_response
```

Ruby

Kit SDK pour Ruby

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signalement des échecs d'articles par lots SQS avec Lambda à l'aide de Ruby.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
require 'json'

def lambda_handler(event:, context:)
  if event
    batch_item_failures = []
```

```
    sqs_batch_response = {}

    event["Records"].each do |record|
      begin
        # process message
      rescue StandardError => e
        batch_item_failures << {"itemIdentifier" => record['messageId']}
      end
    end

    sqs_batch_response["batchItemFailures"] = batch_item_failures
    return sqs_batch_response
  end
end
```

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signalement des échecs d'articles par lots SQS avec Lambda à l'aide de Rust.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
use aws_lambda_events::{
    event::sqs::{SqsBatchResponse, SqsEvent},
    sqs::{BatchItemFailure, SqsMessage},
};
use lambda_runtime::{run, service_fn, Error, LambdaEvent};

async fn process_record(_: &SqsMessage) -> Result<(), Error> {
    Err(Error::from("Error processing message"))
}
```

```
async fn function_handler(event: LambdaEvent<SqsEvent>) ->
 Result<SqsBatchResponse, Error> {
    let mut batch_item_failures = Vec::new();
    for record in event.payload.records {
        match process_record(&record).await {
            Ok(_) => (),
            Err(_) => batch_item_failures.push(BatchItemFailure {
                item_identifier: record.message_id.unwrap(),
            }),
        }
    }

    Ok(SqsBatchResponse {
        batch_item_failures,
    })
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    run(service_fn(function_handler)).await
}
```

Si les événements ayant échoué ne retournent pas dans la file d'attente, voir Comment résoudre les problèmes liés à la fonction Lambda SQS ? ReportBatchItemFailures dans le AWS Knowledge Center.

Conditions de réussite et d’échec

Lambda traite un lot comme un succès complet si votre fonction renvoie l’un des éléments suivants :

- Une liste `batchItemFailures` vide
- Une liste `batchItemFailures` nulle
- Une `EventResponse` vide
- Une `EventResponse` nulle

Lambda traite un lot comme un échec complet si votre fonction renvoie l’un des éléments suivants :

- Une réponse JSON non valide
- Une chaîne `itemIdentifier` vide

- Un `itemIdentifier` nul
- Un `itemIdentifier` avec un nom de clé incorrect
- Une valeur `itemIdentifier` avec un ID de message inexistant

CloudWatch métriques

Pour déterminer si votre fonction signale correctement les défaillances d'articles par lots, vous pouvez surveiller les métriques `NumberOfMessagesDeleted` et `ApproximateAgeOfOldestMessage` Amazon SQS sur Amazon. CloudWatch

- `NumberOfMessagesDeleted` suit le nombre de messages supprimés de votre file d'attente. Si cela tombe à 0, cela indique que la réponse de votre fonction ne renvoie pas correctement les messages d'échec.
- `ApproximateAgeOfOldestMessage` suit combien de temps le message le plus ancien est resté dans votre file d'attente. Une forte augmentation de cette métrique peut indiquer que votre fonction ne renvoie pas correctement les messages d'échec.

Utilisation de Powertools pour AWS Lambda processeur par lots

L'utilitaire de traitement par lots de Powertools for gère AWS Lambda automatiquement la logique de réponse partielle par lots, réduisant ainsi la complexité de la mise en œuvre du signalement des défaillances par lots. Voici des exemples d'utilisation de l'utilitaire de traitement par lots :

Python

> **Note**
>
> Pour des exemples complets et des instructions de configuration, consultez la documentation de l'utilitaire de traitement par lots.

Traitement des messages Amazon SQS à l'aide d'un AWS Lambda traitement par lots.

```
import json
from aws_lambda_powertools import Logger
from aws_lambda_powertools.utilities.batch import BatchProcessor, EventType,
 process_partial_response
from aws_lambda_powertools.utilities.data_classes import SQSEvent
```

```
from aws_lambda_powertools.utilities.typing import LambdaContext

processor = BatchProcessor(event_type=EventType.SQS)
logger = Logger()

def record_handler(record):
    logger.info(record)
    # Your business logic here
    # Raise an exception to mark this record as failed

def lambda_handler(event, context: LambdaContext):
    return process_partial_response(
        event=event,
        record_handler=record_handler,
        processor=processor,
        context=context
    )
```

TypeScript

> **Note**
>
> Pour des exemples complets et des instructions de configuration, consultez la documentation de l'utilitaire de traitement par lots.

Traitement des messages Amazon SQS à l'aide d'un AWS Lambda traitement par lots.

```
import { BatchProcessor, EventType, processPartialResponse } from '@aws-lambda-
powertools/batch';
import { Logger } from '@aws-lambda-powertools/logger';
import type { SQSEvent, Context } from 'aws-lambda';

const processor = new BatchProcessor(EventType.SQS);
const logger = new Logger();

const recordHandler = async (record: any): Promise<void> => {
    logger.info('Processing record', { record });
    // Your business logic here
    // Throw an error to mark this record as failed
};

export const handler = async (event: SQSEvent, context: Context) => {
```

```
    return processPartialResponse(event, recordHandler, processor, {
        context,
    });
};
```

Paramètres Lambda pour les mappages des sources d’événement Amazon SQS

Tous les types de sources d'événements Lambda partagent les mêmes opérations CreateEventSourceMappinget les mêmes opérations d'UpdateEventSourceMappingAPI. Cependant, seuls certains paramètres s’appliquent à Amazon SQS.

Paramètre	Obligatoire	Par défaut	Remarques
BatchSize	N	10	Pour les files d’attente standard, le maximum est de 10 000. Pour les files d’attente FIFO, le maximum est de 10.
Activé	N	VRAI	Aucune
EventSourceArn	O	N/A	ARN du flux de données ou d’un consommateur de flux
FunctionName	O	N/A	Aucune
FilterCriteria	N	N/A	Contrôlez les événements que Lambda envoie à votre fonction d'événement
FunctionResponseTypes	N	N/A	Pour permettre à votre fonction événementielle de signaler des défaillan

Paramètre	Obligatoire	Par défaut	Remarques
			ces spécifiques dans un lot, incluez la valeur `ReportBatchItemFailures` dans `FunctionResponseTypes` . Pour plus d'informations, consultez Mise en œuvre de réponses partielles de lot.
MaximumBatchingWindowInSeconds	N	0	La fenêtre de traitement par lots n'est pas prise en charge pour les files d'attente FIFO
ProvisionedPollerConfig	N	N/A	Configure le nombre minimum (2-200) et maximum (2-2000) de sondeurs d'événements dédiés pour le mappage des sources d'événements SQS. Chaque sondeur peut gérer jusqu'à 1 % MB/sec du débit et 10 appels simultanés.
ScalingConfig	N	N/A	Configuration de la simultanéité maximale pour les sources d'événements Amazon SQS

Utilisation du filtrage des événements avec une source d'événement Amazon SQS

Vous pouvez utiliser le filtrage des événements pour contrôler les enregistrements d'un flux ou d'une file d'attente que Lambda envoie à votre fonction d'événement. Pour obtenir des informations générales sur le fonctionnement du filtrage des événements, consultez the section called "Filtrage des événements".

Cette section porte sur le filtrage des événements pour les sources Amazon SQS.

> **Note**
>
> Les mappages des sources d'événements Amazon SQS prennent uniquement en charge le filtrage sur la clé `body`.

Rubriques

- Notions de base du filtrage des événements Amazon SQS

Notions de base du filtrage des événements Amazon SQS

Supposons que votre file d'attente Amazon SQS contienne des messages au format JSON suivant.

```
{
    "RecordNumber": 1234,
    "TimeStamp": "yyyy-mm-ddThh:mm:ss",
    "RequestCode": "AAAA"
}
```

Un exemple d'enregistrement pour cette file d'attente ressemblerait à ce qui suit.

```
{
    "messageId": "059f36b4-87a3-44ab-83d2-661975830a7d",
    "receiptHandle": "AQEBwJnKyrHigUMZj6rYigCgxlaS3SLy0a...",
    "body": "{\n "RecordNumber": 1234,\n "TimeStamp": "yyyy-mm-ddThh:mm:ss",\n
 "RequestCode": "AAAA"\n}",
    "attributes": {
        "ApproximateReceiveCount": "1",
        "SentTimestamp": "1545082649183",
        "SenderId": "AIDAIENQZJOLO23YVJ4VO",
```

```
        "ApproximateFirstReceiveTimestamp": "1545082649185"
        },
    "messageAttributes": {},
    "md5OfBody": "e4e68fb7bd0e697a0ae8f1bb342846b3",
    "eventSource": "aws:sqs",
    "eventSourceARN": "arn:aws:sqs:us-west-2:123456789012:my-queue",
    "awsRegion": "us-west-2"
}
```

Pour filtrer en fonction du contenu de vos messages Amazon SQS, utilisez la clé `body` dans l'enregistrement du message Amazon SQS. Supposons que vous souhaitiez traiter uniquement les enregistrements pour lesquels `RequestCode` le message Amazon SQS est « BBBB ». L'objet `FilterCriteria` serait le suivant.

```
{
    "Filters": [
        {
            "Pattern": "{ \"body\" : { \"RequestCode\" : [ \"BBBB\" ] } }"
        }
    ]
}
```

Pour plus de clarté, voici la valeur du `Pattern` de filtre étendu en JSON simple :

```
{
    "body": {
        "RequestCode": [ "BBBB" ]
        }
}
```

Vous pouvez ajouter votre filtre à l'aide de la console AWS CLI ou d'un AWS SAM modèle.

Console

Pour ajouter ce filtre à l'aide de la console, suivez les instructions de Attacher des critères de filtre à un mappage de sources d'événements (console) et saisissez la chaîne suivante comme critère de filtre.

```
{ "body" : { "RequestCode" : [ "BBBB" ] } }
```

AWS CLI

Pour créer un nouveau mappage de source d'événements avec ces critères de filtre à l'aide de AWS Command Line Interface (AWS CLI), exécutez la commande suivante.

```
aws lambda create-event-source-mapping \
    --function-name my-function \
    --event-source-arn arn:aws:sqs:us-east-2:123456789012:my-queue \
    --filter-criteria '{"Filters": [{"Pattern": "{ \"body\" : { \"RequestCode\" :
 [ \"BBBB\" ] } }"}]}'
```

Pour ajouter ces critères de filtre à un mappage des sources d'événements existant, exécutez la commande suivante.

```
aws lambda update-event-source-mapping \
    --uuid "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE" \
    --filter-criteria '{"Filters": [{"Pattern": "{ \"body\" : { \"RequestCode\" :
 [ \"BBBB\" ] } }"}]}'
```

AWS SAM

Pour ajouter ce filtre AWS SAM, ajoutez l'extrait suivant au modèle YAML de votre source d'événement.

```
FilterCriteria:
  Filters:
    - Pattern: '{ "body" : { "RequestCode" : [ "BBBB" ] } }'
```

Supposons que vous souhaitiez que votre fonction d'événement traite uniquement les enregistrements dont la `RecordNumber` valeur est supérieure à 9999. L'objet `FilterCriteria` serait le suivant.

```
{
    "Filters": [
        {
            "Pattern": "{ \"body\" : { \"RecordNumber\" : [ { \"numeric\": [ \">\",
 9999 ] } ] } }"
        }
    ]
}
```

Pour plus de clarté, voici la valeur du `Pattern` de filtre étendu en JSON simple :

```
{
    "body": {
        "RecordNumber": [
            {
                "numeric": [ ">", 9999 ]
            }
        ]
    }
}
```

Vous pouvez ajouter votre filtre à l'aide de la console AWS CLI ou d'un AWS SAM modèle.

Console

Pour ajouter ce filtre à l'aide de la console, suivez les instructions de Attacher des critères de filtre à un mappage de sources d'événements (console) et saisissez la chaîne suivante comme critère de filtre.

```
{ "body" : { "RecordNumber" : [ { "numeric": [ ">", 9999 ] } ] } }
```

AWS CLI

Pour créer un nouveau mappage de source d'événements avec ces critères de filtre à l'aide de AWS Command Line Interface (AWS CLI), exécutez la commande suivante.

```
aws lambda create-event-source-mapping \
    --function-name my-function \
    --event-source-arn arn:aws:sqs:us-east-2:123456789012:my-queue \
    --filter-criteria '{"Filters": [{"Pattern": "{ \"body\" : { \"RecordNumber\" :
 [ { \"numeric\": [ \">\", 9999 ] } ] } }"}]}'
```

Pour ajouter ces critères de filtre à un mappage des sources d'événements existant, exécutez la commande suivante.

```
aws lambda update-event-source-mapping \
    --uuid "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE" \
    --filter-criteria '{"Filters": [{"Pattern": "{ \"body\" : { \"RecordNumber\" :
 [ { \"numeric\": [ \">\", 9999 ] } ] } }"}]}'
```

AWS SAM

Pour ajouter ce filtre AWS SAM, ajoutez l'extrait suivant au modèle YAML de votre source d'événement.

```
FilterCriteria:
  Filters:
    - Pattern: '{ "body" : { "RecordNumber" : [ { "numeric": [ ">", 9999 ] } ] } }'
```

Pour Amazon SQS, le corps du message peut être n'importe quelle chaîne. Toutefois, cela peut être problématique si votre `FilterCriteria` s'attend à ce que `body` se présente dans un format JSON valide. Le scénario inverse est également vrai, si le corps du message entrant est au format JSON, mais que votre critère de filtre s'attend à ce que `body` soit une chaîne de texte brut, cela peut entraîner un comportement inattendu.

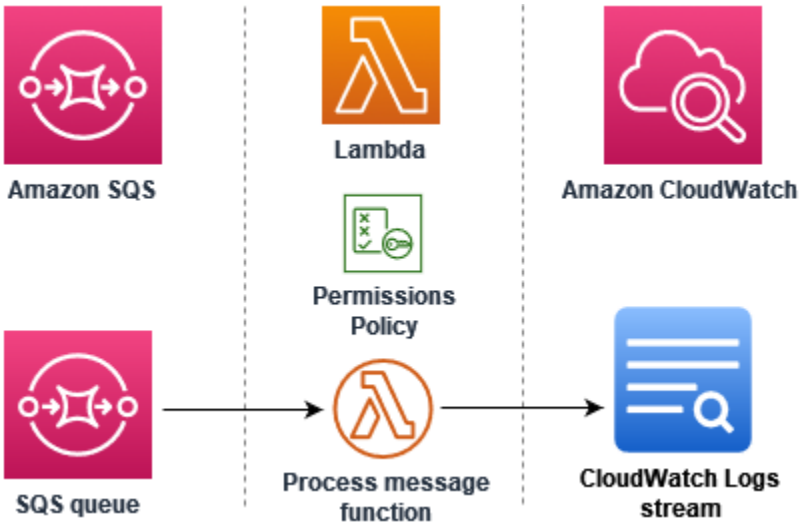
Pour éviter ce problème, assurez-vous que le format du corps dans vos `FilterCriteria` correspond au format attendu de `body` dans les messages que vous recevez de votre file d'attente. Avant de filtrer vos messages, Lambda évalue automatiquement le format du corps de votre message entrant et de votre modèle de filtre pour `body`. En cas de décalage, Lambda abandonne le message. Le tableau suivant résume cette évaluation :

Format du **body** du message entrant	Format du **body** du modèle de filtre	Action obtenue.
Chaîne de texte brut	Chaîne de texte brut	Lambda filtre en fonction de vos critères de filtre.
Chaîne de texte brut	Pas de modèle de filtre pour les propriétés des données	Lambda filtre (uniquement selon les autres propriétés de métadonnées) en fonction de vos critères de filtre.
Chaîne de texte brut	JSON valide	Lambda rejette le message.
JSON valide	Chaîne de texte brut	Lambda rejette le message.
JSON valide	Pas de modèle de filtre pour les propriétés des données	Lambda filtre (uniquement selon les autres propriétés de

Format du **body** du message entrant	Format du **body** du modèle de filtre	Action obtenue.
		métadonnées) en fonction de vos critères de filtre.
JSON valide	JSON valide	Lambda filtre en fonction de vos critères de filtre.

Didacticiel : utilisation de Lambda avec Amazon SQS

Dans ce didacticiel, vous allez créer une fonction d'événement Lambda qui consomme les messages d'une file d'attente Amazon Simple Queue Service (Amazon SQS). La fonction d'événement Lambda s'exécute chaque fois qu'un nouveau message est ajouté à la file d'attente. La fonction écrit les messages dans un flux Amazon CloudWatch Logs. Le diagramme suivant montre les ressources AWS utilisées pour compléter ce tutoriel.



Pour compléter ce didacticiel, effectuez les tâches suivantes :

1. Créez une fonction d'événement Lambda qui écrit des messages dans des journaux. CloudWatch
2. Créer une file d’attente Amazon SQS.
3. Créez un mappage des sources d’événements Lambda. Le mappage des sources d'événements lit la file d'attente Amazon SQS et appelle votre fonction d'événement Lambda lorsqu'un nouveau message est ajouté.

4. Testez la configuration en ajoutant des messages à votre file d'attente et en surveillant les résultats dans CloudWatch Logs.

Conditions préalables

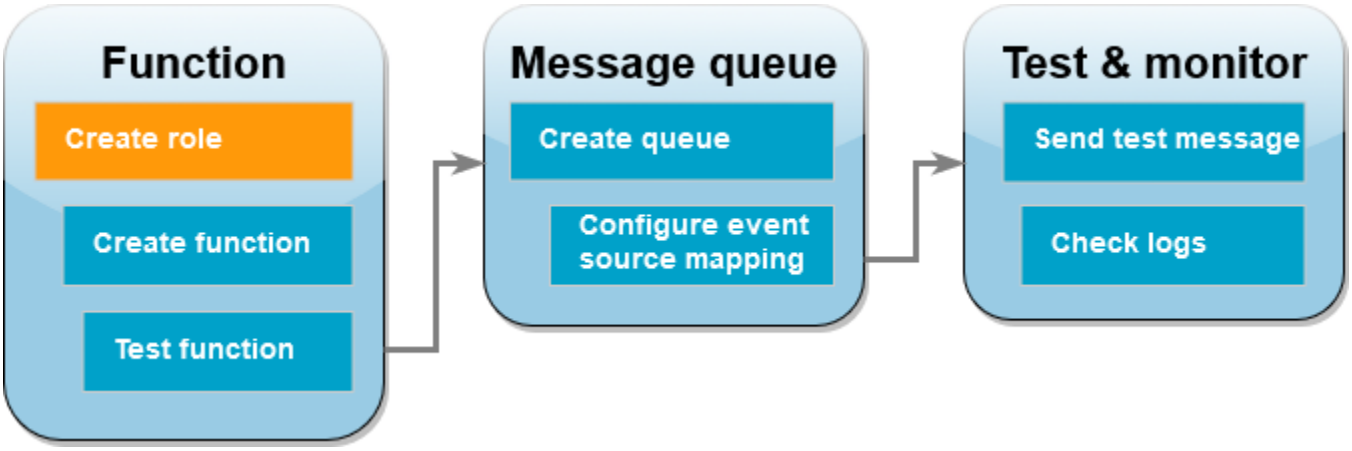
Installer la AWS Command Line Interface

Si vous ne l'avez pas encore installé AWS Command Line Interface, suivez les étapes décrites dans la section Installation ou mise à jour de la dernière version du AWS CLI pour l'installer.

Ce tutoriel nécessite un terminal de ligne de commande ou un shell pour exécuter les commandes. Sous Linux et macOS, utilisez votre gestionnaire de shell et de package préféré.

> **Note**
>
> Sous Windows, certaines commandes CLI Bash que vous utilisez couramment avec Lambda (par exemple `zip`) ne sont pas prises en charge par les terminaux intégrés du système d'exploitation. Pour obtenir une Windows-integrated version d'Ubuntu et de Bash, installez le sous-système Windows pour Linux.

Créer le rôle d'exécution



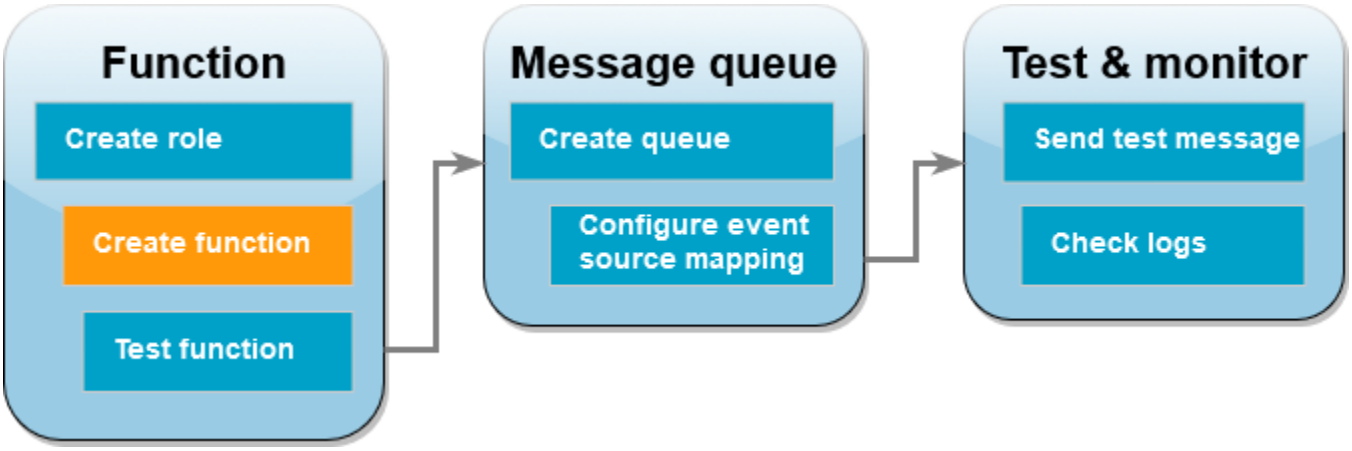
Un rôle d'exécution est un rôle Gestion des identités et des accès AWS (IAM) qui accorde à une fonction d'événement Lambda l'autorisation d' Services AWS accès et de ressources. Pour permettre à votre fonction de lire des éléments depuis Amazon SQS, joignez la politique d'AWSLambdaSQSQueueExecutionRoleautorisation.

Pour créer un rôle d'exécution et attacher une politique d'autorisations Amazon SQS

1. Ouvrez la page Rôles de la console IAM.
2. Sélectionnez Créer un rôle.
3. Pour Type d'entité de confiance, choisissez Service AWS .
4. Pour Cas d'utilisation, choisissez Lambda.
5. Choisissez Suivant.
6. Dans le champ de recherche Politiques d'autorisations, saisissez **`AWSLambdaSQSQueueExecutionRole`**.
7. Sélectionnez la AWSLambdaSQSQueueExecutionRolepolitique, puis cliquez sur Suivant.
8. Sous Détails du rôle, pour Nom du rôle, saisissez **`lambda-sqs-role`**, puis sélectionnez Créer un rôle.

Après la création du rôle, notez l'Amazon Resource Name (ARN) de votre rôle d'exécution. Vous en aurez besoin dans les étapes suivantes.

Création de la fonction d'événement



Créez une fonction d'événement Lambda qui traite vos messages Amazon SQS. Le code de fonction enregistre le corps du message Amazon SQS dans Logs. CloudWatch

Ce didacticiel utilise le runtime Node.js 24, mais nous avons également fourni des exemples de code dans d'autres langages d'exécution. Vous pouvez sélectionner l'onglet dans la zone suivante pour voir le code de l'exécution qui vous intéresse. Le JavaScript code que vous allez utiliser dans cette étape se trouve dans le premier exemple présenté dans l'JavaScriptonglet.

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Utilisation d'un événement SQS avec Lambda en utilisant .NET.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
using Amazon.Lambda.Core;
using Amazon.Lambda.SQSEvents;


// Assembly attribute to enable the Lambda function's JSON input to be converted
 into a .NET class.
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSeri

namespace SqsIntegrationSampleCode
{
    public async Task FunctionHandler(SQSEvent evnt, ILambdaContext context)
    {
        foreach (var message in evnt.Records)
        {
            await ProcessMessageAsync(message, context);
        }

        context.Logger.LogInformation("done");
    }

    private async Task ProcessMessageAsync(SQSEvent.SQSMessage message,
 ILambdaContext context)
    {
        try
        {
            context.Logger.LogInformation($"Processed message {message.Body}");

            // TODO: Do interesting work based on the new message
```

```
            await Task.CompletedTask;
        }
        catch (Exception e)
        {
            //You can use Dead Letter Queue to handle failures. By configuring a
 Lambda DLQ.
            context.Logger.LogError($"An error occurred");
            throw;
        }

    }
}
```

Go

Kit SDK pour Go V2

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement SQS avec Lambda à l'aide de Go.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package integration_sqs_to_lambda

import (
 "fmt"
 "github.com/aws/aws-lambda-go/events"
 "github.com/aws/aws-lambda-go/lambda"
)

func handler(event events.SQSEvent) error {
 for _, record := range event.Records {
  err := processMessage(record)
  if err != nil {
   return err
  }
```

```
 }
 fmt.Println("done")
 return nil
}

func processMessage(record events.SQSMessage) error {
 fmt.Printf("Processed message %s\n", record.Body)
 // TODO: Do interesting work based on the new message
 return nil
}

func main() {
 lambda.Start(handler)
}
```

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Utilisation d'un événement SQS avec Lambda à l'aide de Java.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.SQSEvent;
import com.amazonaws.services.lambda.runtime.events.SQSEvent.SQSMessage;

public class Function implements RequestHandler<SQSEvent, Void> {
    @Override
    public Void handleRequest(SQSEvent sqsEvent, Context context) {
        for (SQSMessage msg : sqsEvent.getRecords()) {
            processMessage(msg, context);
        }
        context.getLogger().log("done");
```

```
        return null;
    }

    private void processMessage(SQSMessage msg, Context context) {
        try {
            context.getLogger().log("Processed message " + msg.getBody());

            // TODO: Do interesting work based on the new message

        } catch (Exception e) {
            context.getLogger().log("An error occurred");
            throw e;
        }

    }
}
```

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement SQS avec JavaScript Lambda en utilisant.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
exports.handler = async (event, context) => {
  for (const message of event.Records) {
    await processMessageAsync(message);
  }
  console.info("done");
};

async function processMessageAsync(message) {
  try {
    console.log(`Processed message ${message.body}`);
    // TODO: Do interesting work based on the new message
```

```
    await Promise.resolve(1); //Placeholder for actual async work
  } catch (err) {
    console.error("An error occurred");
    throw err;
  }
}
```

Consommation d'un événement SQS avec TypeScript Lambda en utilisant.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import { SQSEvent, Context, SQSHandler, SQSRecord } from "aws-lambda";

export const functionHandler: SQSHandler = async (
  event: SQSEvent,
  context: Context
): Promise<void> => {
  for (const message of event.Records) {
    await processMessageAsync(message);
  }
  console.info("done");
};

async function processMessageAsync(message: SQSRecord): Promise<any> {
  try {
    console.log(`Processed message ${message.body}`);
    // TODO: Do interesting work based on the new message
    await Promise.resolve(1); //Placeholder for actual async work
  } catch (err) {
    console.error("An error occurred");
    throw err;
  }
}
```

PHP

Kit SDK pour PHP

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement SQS avec Lambda à l'aide de PHP.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
<?php

# using bref/bref and bref/logger for simplicity

use Bref\Context\Context;
use Bref\Event\InvalidLambdaEvent;
use Bref\Event\Sqs\SqsEvent;
use Bref\Event\Sqs\SqsHandler;
use Bref\Logger\StderrLogger;

require __DIR__ . '/vendor/autoload.php';

class Handler extends SqsHandler
{
    private StderrLogger $logger;
    public function __construct(StderrLogger $logger)
    {
        $this->logger = $logger;
    }

    /**
     * @throws InvalidLambdaEvent
     */
    public function handleSqs(SqsEvent $event, Context $context): void
    {
        foreach ($event->getRecords() as $record) {
            $body = $record->getBody();
            // TODO: Do interesting work based on the new message
        }
```

```
    }
}

$logger = new StderrLogger();
return new Handler($logger);
```

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Utilisation d'un événement SQS avec Lambda à l'aide de Python.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
def lambda_handler(event, context):
    for message in event['Records']:
        process_message(message)
    print("done")

def process_message(message):
    try:
        print(f"Processed message {message['body']}")
        # TODO: Do interesting work based on the new message
    except Exception as err:
        print("An error occurred")
        raise err
```

Ruby

Kit SDK pour Ruby

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Utilisation d'un événement SQS avec Lambda à l'aide de Ruby.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
def lambda_handler(event:, context:)
  event['Records'].each do |message|
    process_message(message)
  end
  puts "done"
end

def process_message(message)
  begin
    puts "Processed message #{message['body']}"
    # TODO: Do interesting work based on the new message
  rescue StandardError => err
    puts "An error occurred"
    raise err
  end
end
```

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement SQS avec Lambda à l'aide de Rust.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
use aws_lambda_events::event::sqs::SqsEvent;
use lambda_runtime::{run, service_fn, Error, LambdaEvent};

async fn function_handler(event: LambdaEvent<SqsEvent>) -> Result<(), Error> {
    event.payload.records.iter().for_each(|record| {
        // process the record
        tracing::info!("Message body: {}",
 record.body.as_deref().unwrap_or_default())
    });

    Ok(())
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    tracing_subscriber::fmt()
        .with_max_level(tracing::Level::INFO)
        // disable printing the name of the module in every log line.
        .with_target(false)
        // disabling time is handy because CloudWatch will add the ingestion
 time.
        .without_time()
        .init();

    run(service_fn(function_handler)).await
}
```

Pour créer une fonction d' Node.js événement Lambda

1. Créez un répertoire pour le projet, puis passez à ce répertoire.

```
mkdir sqs-tutorial
cd sqs-tutorial
```

2. Copiez l'exemple de JavaScript code dans un nouveau fichier nomméindex.js.
3. Créez un package de déploiement à l'aide de la commande zip suivante.

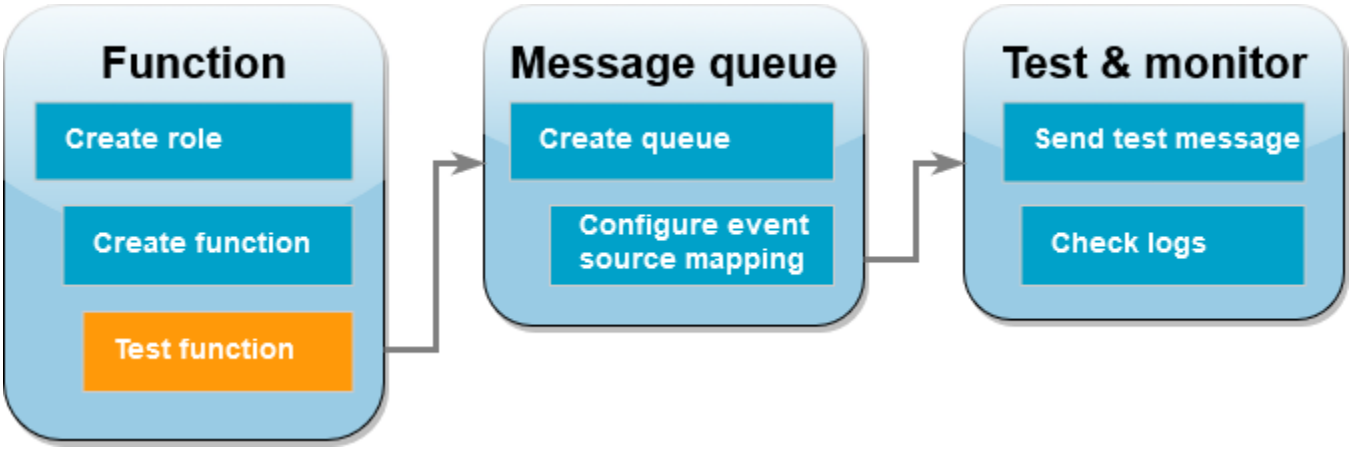
```
zip function.zip index.js
```

4. Créez une fonction d'événement Lambda à l'aide de la commande AWS CLI create-function. Pour le paramètre `role`, entrez l'ARN du rôle d'exécution que vous avez créé précédemment.

> **Note**
>
> La fonction d'événement Lambda et la file d'attente Amazon SQS doivent être identiques. Région AWS

```
aws lambda create-function --function-name ProcessSQSRecord \
--zip-file fileb://function.zip --handler index.handler --runtime nodejs24.x \
--role arn:aws:iam::111122223333:role/lambda-sqs-role
```

Tester la fonction d'événement



Appelez votre fonction d'événement Lambda manuellement à l'aide de la `invoke` AWS CLI commande et d'un exemple d'événement Amazon SQS.

Pour appeler la fonction d'événement Lambda avec un exemple d'événement

1. Enregistrez le JSON suivant en tant que fichier nommé `input.json`. Ce JSON simule un événement qu'Amazon SQS pourrait envoyer à votre fonction d'événement Lambda, `"body"` où il contient le message réel provenant de la file d'attente. Dans cet exemple, le message est `"test"`.

ExampleÉvénement Amazon SQS

Il s'agit d'un événement de test : vous n'avez pas besoin de modifier le message ou le numéro de compte.

```
{
    "Records": [
        {
            "messageId": "059f36b4-87a3-44ab-83d2-661975830a7d",
            "receiptHandle": "AQEBwJnKyrHigUMZj6rYigCgxlaS3SLy0a...",
            "body": "test",
            "attributes": {
                "ApproximateReceiveCount": "1",
                "SentTimestamp": "1545082649183",
                "SenderId": "AIDAIENQZJOLO23YVJ4VO",
                "ApproximateFirstReceiveTimestamp": "1545082649185"
            },
            "messageAttributes": {},
            "md5OfBody": "098f6bcd4621d373cade4e832627b4f6",
            "eventSource": "aws:sqs",
            "eventSourceARN": "arn:aws:sqs:us-east-1:111122223333:my-queue",
            "awsRegion": "us-east-1"
        }
    ]
}
```

2. Exécutez la AWS CLI commande d'appel suivante. Cette commande renvoie CloudWatch les journaux dans la réponse. Pour de plus amples informations sur la récupération des journaux, veuillez consulter Accédez aux journaux avec AWS CLI.

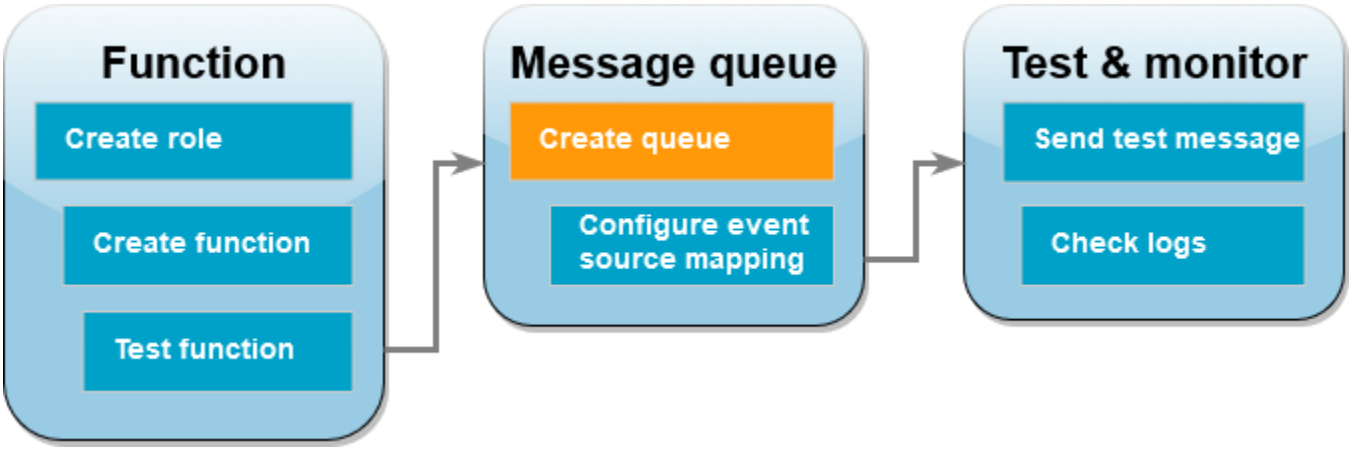
```
aws lambda invoke --function-name ProcessSQSRecord --payload file://input.json out
 --log-type Tail \
--query 'LogResult' --output text --cli-binary-format raw-in-base64-out | base64 --
decode
```

L'cli-binary-formatoption est obligatoire si vous utilisez AWS CLI la version 2. Pour faire de ce paramètre le paramètre par défaut, exécutez `aws configure set cli-binary-format raw-in-base64-out`. Pour plus d'informations, consultez les options de ligne de commande globales prises en charge par l'AWS CLI dans le Guide de l'utilisateur AWS Command Line Interface version 2.

3. Recherchez le journal `INFO` dans la réponse. C'est ici que la fonction d'événement Lambda enregistre le corps du message. Vous devriez voir des journaux qui ressemblent à ceci :

```
2023-09-11T22:45:04.271Z 348529ce-2211-4222-9099-59d07d837b60 INFO Processed
 message test
2023-09-11T22:45:04.288Z 348529ce-2211-4222-9099-59d07d837b60 INFO done
```

Créez une file d’attente Amazon SQS.



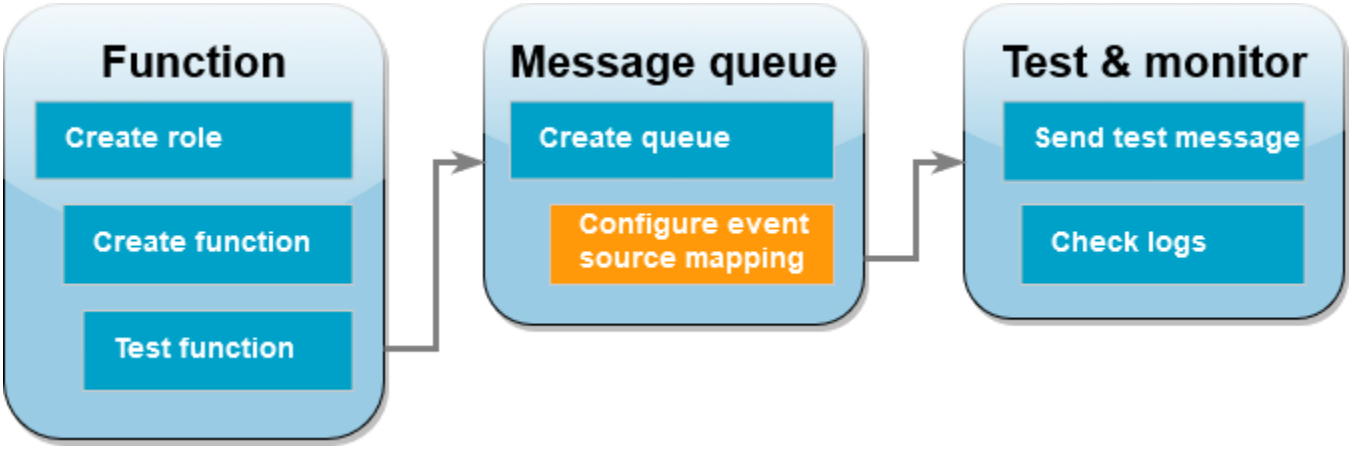
Créez une file d'attente Amazon SQS que la fonction d'événement Lambda peut utiliser comme source d'événements. La fonction d'événement Lambda et la file d'attente Amazon SQS doivent être identiques. Région AWS

Pour créer une file d’attente

1. Ouvrez la console Amazon SQS.
2. Choisissez Créez une file d’attente.
3. Entrez un nom pour la queue. Conservez les paramètres par défaut de toutes les autres options.
4. Choisissez Créez une file d’attente.

Une fois la file d’attente créée, notez son ARN. Vous en aurez besoin à l'étape suivante lorsque vous associerez la file d'attente à votre fonction d'événement Lambda.

Configurer la source de l'événement



Connectez la file d'attente Amazon SQS à votre fonction d'événement Lambda en créant un mappage de source d'événements. Le mappage des sources d'événements lit la file d'attente Amazon SQS et appelle votre fonction d'événement Lambda lorsqu'un nouveau message est ajouté.

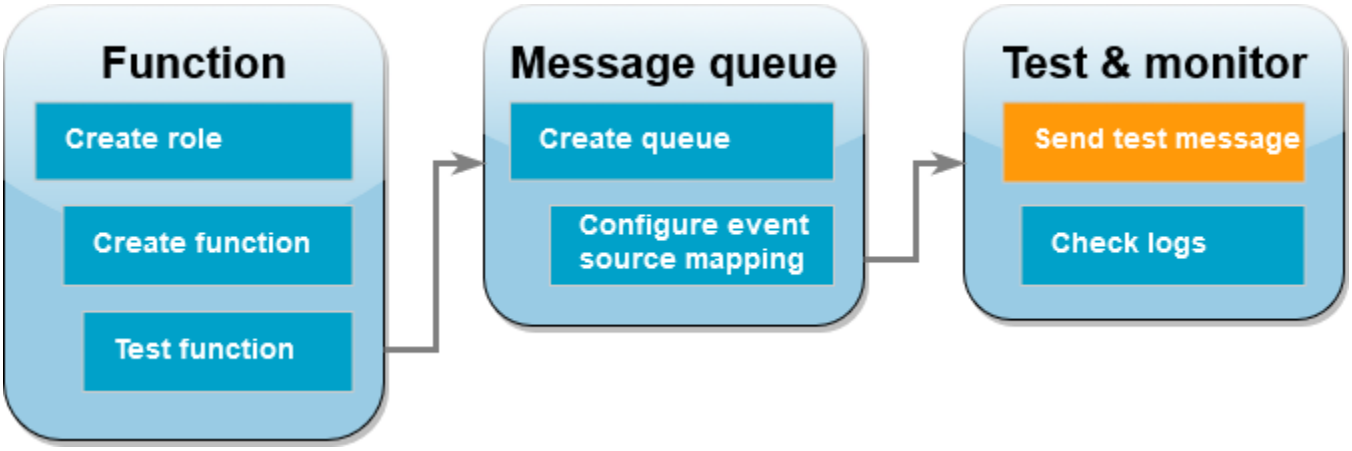
Pour créer un mappage entre votre file d'attente Amazon SQS et votre fonction d'événement Lambda, utilisez la commande create-event-source-mapping. AWS CLI Exemple :

```
aws lambda create-event-source-mapping --function-name ProcessSQSRecord  --batch-size
 10 \
--event-source-arn arn:aws:sqs:us-east-1:111122223333:my-queue
```

Pour obtenir la liste de vos mappages des sources d'événements, utilisez la commande list-event-source-mappings. Exemple :

```
aws lambda list-event-source-mappings --function-name ProcessSQSRecord
```

Envoyer un message de test

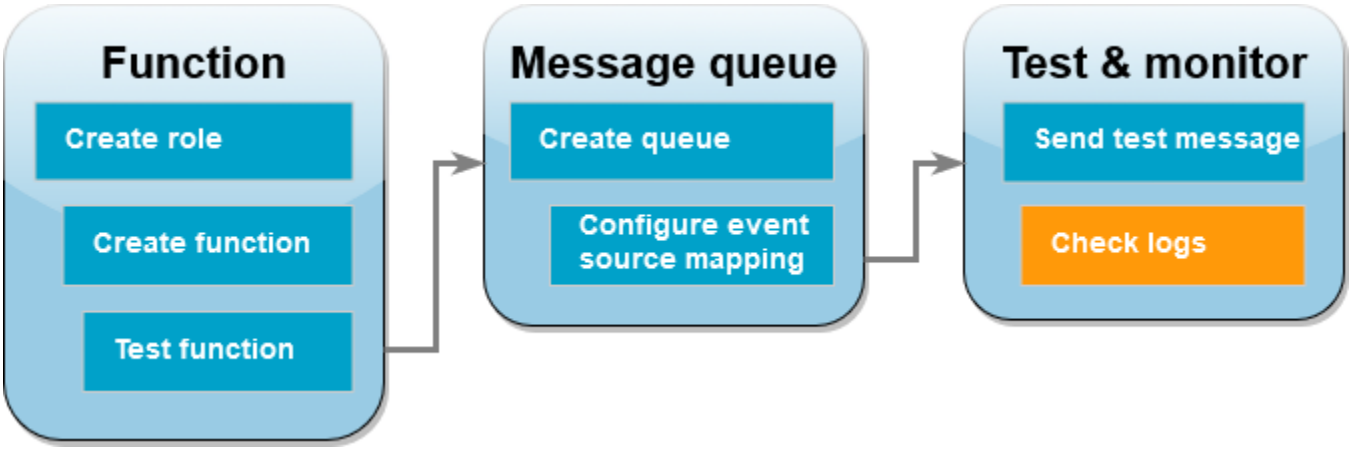


Pour envoyer un message Amazon SQS à la fonction d'événement Lambda

1. Ouvrez la console Amazon SQS.
2. Choisissez la queue que vous avez créée précédemment.
3. Choisissez Envoyer et recevoir des messages.
4. Sous Corps du message, entrez un message de test, tel que « ceci est un message de test ».
5. Choisissez Send Message (Envoyer un message).

Lambda interroge la file d'attente concernant les mises à jour. Lorsqu'il y a un nouveau message, Lambda invoque votre fonction avec ces nouvelles données d'événement de la file d'attente. Si le gestionnaire de la fonction revient sans exception, Lambda considère le message comme traité avec succès et commence à lire de nouveaux messages dans la file d'attente. Après avoir traité un message avec succès, Lambda le supprime automatiquement de la file d'attente. Si le gestionnaire renvoie une exception, Lambda considère que le traitement du lot de messages a échoué et invoque la fonction avec le même lot de messages.

Consultez les CloudWatch journaux



Pour confirmer que la fonction événementielle a traité le message

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez la fonction ProcessSQSRecord.
3. Sélectionnez Monitor (Surveiller).
4. Choisissez Afficher CloudWatch les journaux.
5. Dans la CloudWatch console, choisissez le flux de log pour la fonction.

6. Recherchez le journal `INFO`. C'est ici que la fonction d'événement Lambda enregistre le corps du message. Vous devriez voir le message que vous avez envoyé depuis la file d'attente Amazon SQS. Exemple :

```
2023-09-11T22:49:12.730Z b0c41e9c-0556-5a8b-af83-43e59efeec71 INFO Processed
 message this is a test message.
```

Nettoyage de vos ressources

Vous pouvez maintenant supprimer les ressources que vous avez créées pour ce didacticiel, sauf si vous souhaitez les conserver. En supprimant AWS les ressources que vous n'utilisez plus, vous évitez des frais inutiles pour votre Compte AWS.

Pour supprimer le rôle d'exécution

1. Ouvrez la page Roles (Rôles) de la console IAM.
2. Sélectionnez le rôle d'exécution que vous avez créé.
3. Sélectionnez Supprimer.
4. Saisissez le nom du rôle dans le champ de saisie de texte et choisissez Delete (Supprimer).

Pour supprimer la fonction d'événement Lambda

1. Ouvrez la page Event Functions de la console Lambda.
2. Sélectionnez la fonction d'événement que vous avez créée.
3. Sélectionnez Actions, Supprimer.
4. Saisissez **`confirm`** dans la zone de saisie de texte et choisissez Delete (Supprimer).

Pour supprimer la file d'attente Amazon SQS

1. Connectez-vous à la console Amazon SQS Console de gestion AWS et ouvrez-la à l'adresse. https://console.aws.amazon.com/sqs/
2. Sélectionnez la file d'attente que vous avez créée.
3. Sélectionnez Supprimer.
4. Saisissez **`confirm`** dans le champ de saisie de texte.
5. Sélectionnez Supprimer.

Didacticiel : utilisation d'une file d'attente Amazon SQS entre comptes en tant que source d'événement

Dans ce didacticiel, vous allez créer une fonction d'événement Lambda qui consomme les messages d'une file d'attente Amazon Simple Queue Service (Amazon SQS) d'un autre compte. AWS Ce didacticiel implique deux AWS comptes : le compte A fait référence au compte qui contient votre fonction d'événement Lambda, et le compte B fait référence au compte qui contient la file d'attente Amazon SQS.

Conditions préalables

Installer la AWS Command Line Interface

Si vous ne l'avez pas encore installé AWS Command Line Interface, suivez les étapes décrites dans la section Installation ou mise à jour de la dernière version du AWS CLI pour l'installer.

Ce tutoriel nécessite un terminal de ligne de commande ou un shell pour exécuter les commandes. Sous Linux et macOS, utilisez votre gestionnaire de shell et de package préféré.

> **Note**
>
> Sous Windows, certaines commandes CLI Bash que vous utilisez couramment avec Lambda (par exemple `zip`) ne sont pas prises en charge par les terminaux intégrés du système d'exploitation. Pour obtenir une Windows-integrated version d'Ubuntu et de Bash, installez le sous-système Windows pour Linux.

Création du rôle d'exécution (compte A)

Dans le compte A, créez un rôle d'exécution qui autorise votre fonction à accéder aux AWS ressources requises.

Pour créer un rôle d'exécution

1. Ouvrez la page Rôles dans la console Gestion des identités et des accès AWS (IAM).
2. Choisissez Créer un rôle.
3. Créez un rôle avec les propriétés suivantes :
   - Trusted entity (Entité de confiance) – AWS Lambda.
   - Permissions (Autorisations – AWSLambdaSQSQueueExecutionRole

- Nom de rôle – **`cross-account-lambda-sqs-role`**

La AWSLambdaSQSQueueExecutionRolepolitique dispose des autorisations dont la fonction a besoin pour lire des éléments depuis Amazon SQS et pour écrire des journaux dans Amazon CloudWatch Logs.

Création de la fonction d'événement (compte A)

Dans le compte A, créez une fonction d'événement Lambda qui traite vos messages Amazon SQS. La fonction d'événement Lambda et la file d'attente Amazon SQS doivent être identiques. Région AWS

L'exemple de Node.js code suivant écrit chaque message dans CloudWatch un journal de connexion.

Example index.mjs

```
export const handler = async function(event, context) {
  event.Records.forEach(record => {
    const { body } = record;
    console.log(body);
  });
  return {};
}
```

Pour créer la fonction d'événement

> **Note**
>
> Suivez ces étapes pour créer une Node.js fonction. Pour les autres langages, les étapes sont similaires mais certains détails sont différents.

1. Enregistrez l'exemple de code en tant que fichier nommé `index.mjs`.
2. Créez un package de déploiement.

   ```
   zip function.zip index.mjs
   ```

3. Créez la fonction à l'aide de la commande `create-function` AWS Command Line Interface (AWS CLI). Remplacez `arn:aws:iam::111122223333:role/cross-account-lambda-sqs-role` par l'ARN du rôle d'exécution que vous avez créé auparavant.

```
aws lambda create-function --function-name CrossAccountSQSExample \
--zip-file fileb://function.zip --handler index.handler --runtime nodejs24.x \
--role arn:aws:iam::111122223333:role/cross-account-lambda-sqs-role
```

Tester la fonction d'événement (compte A)

Dans le compte A, testez manuellement votre fonction d'événement Lambda à l'aide de la `invoke` AWS CLI commande et d'un exemple d'événement Amazon SQS.

Si le gestionnaire revient normalement sans exception, Lambda considère le message comme traité avec succès et commence à lire de nouveaux messages dans la file d'attente. Après avoir traité un message avec succès, Lambda le supprime automatiquement de la file d'attente. Si le gestionnaire renvoie une exception, Lambda considère que le traitement du lot de messages a échoué et invoque la fonction avec le même lot de messages.

1. Enregistrez le JSON suivant en tant que fichier nommé `input.txt`.

```
{
    "Records": [
        {
            "messageId": "059f36b4-87a3-44ab-83d2-661975830a7d",
            "receiptHandle": "AQEBwJnKyrHigUMZj6rYigCgxlaS3SLy0a...",
            "body": "test",
            "attributes": {
                "ApproximateReceiveCount": "1",
                "SentTimestamp": "1545082649183",
                "SenderId": "AIDAIENQZJOLO23YVJ4VO",
                "ApproximateFirstReceiveTimestamp": "1545082649185"
            },
            "messageAttributes": {},
            "md5OfBody": "098f6bcd4621d373cade4e832627b4f6",
            "eventSource": "aws:sqs",
            "eventSourceARN": "arn:aws:sqs:us-east-1:111122223333:example-queue",
            "awsRegion": "us-east-1"
        }
    ]
}
```

Le JSON précédent simule un événement qu'Amazon SQS pourrait envoyer à votre fonction d'événement Lambda, `"body"` où il contient le message réel provenant de la file d'attente.

2. Exécutez la commande suivante `invoke` AWS CLI .

```
aws lambda invoke --function-name CrossAccountSQSExample \
--cli-binary-format raw-in-base64-out \
--payload file://input.txt outputfile.txt
```

L'cli-binary-formatoption est obligatoire si vous utilisez AWS CLI la version 2. Pour faire de ce paramètre le paramètre par défaut, exécutez `aws configure set cli-binary-format raw-in-base64-out`. Pour plus d'informations, consultez les options de ligne de commande globales AWS CLI prises en charge dans le Guide de l'utilisateur AWS Command Line Interface version 2.

3. Vérifiez la sortie dans le fichier `outputfile.txt`.

Créer une file d'attente Amazon SQS (Compte B)

Dans le compte B, créez une file d'attente Amazon SQS que la fonction d'événement Lambda du compte A peut utiliser comme source d'événements. La fonction d'événement Lambda et la file d'attente Amazon SQS doivent être identiques. Région AWS

Pour créer une file d'attente

1. Ouvrez la console Amazon SQS.
2. Choisissez Créez une file d'attente.
3. Créez une fille d'attente avec les propriétés suivantes.
   - Type–Standard
   - Nom – LambdaCrossAccountQueue
   - Configuration— Conservez les paramètres par défaut.
   - Stratégie d'accès – Choisissez Avancé. Collez dans la stratégie JSON suivante. Remplacez les valeurs suivantes :
     - `111122223333`: Compte AWS ID du compte A
     - `444455556666`: Compte AWS ID du compte B

     JSON

```
{
    "Version":"2012-10-17",
```

```
    "Id": "Queue1_Policy_UUID",
    "Statement": [
        {
            "Sid": "Queue1_AllActions",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:role/cross-account-lambda-
sqs-role"
                ]
            },
            "Action": "sqs:*",
            "Resource": "arn:aws:sqs:us-
east-1:444455556666:LambdaCrossAccountQueue"
        }
    ]
}
```

Cette stratégie accorde au rôle d'exécution Lambda dansCompte Aautorisations pour consommer des messages de cette file d'attente Amazon SQS.

4. Après avoir créé la file d'attente, enregistrez son Amazon Resource Name (ARN). Vous en aurez besoin à l'étape suivante lorsque vous associerez la file d'attente à votre fonction d'événement Lambda.

Configurer la source de l'événement (Compte A)

Dans le compte A, créez un mappage de source d'événement entre la file d'attente Amazon SQS du compte B et votre fonction d'événement Lambda en exécutant la commande suivante. `create-event-source-mapping` AWS CLI Remplacez `arn:aws:sqs:us-east-1:444455556666:LambdaCrossAccountQueue` par l'ARN de la file d'attente Amazon SQS que vous avez créée à l'étape précédente.

```
aws lambda create-event-source-mapping --function-name CrossAccountSQSExample --batch-
size 10 \
--event-source-arn arn:aws:sqs:us-east-1:444455556666:LambdaCrossAccountQueue
```

Pour obtenir une liste de vos mappages de source d'événements, exécutez la commande suivante.

```
aws lambda list-event-source-mappings --function-name CrossAccountSQSExample \
--event-source-arn arn:aws:sqs:us-east-1:444455556666:LambdaCrossAccountQueue
```

Tester la configuration

Maintenant, vous pouvez tester la configuration comme suit :

1. DansCompte B, ouvrezConsole Amazon SQS.
2. Choisissez LambdaCrossAccountQueuecelui que vous avez créé précédemment.
3. Choisissez Send and receive messages (Envoyer et recevoir des messages).
4. Sous Message body (Corps du message), saisissez un message test.
5. Choisissez Send Message (Envoyer un message).

Votre fonction d'événement Lambda dans le compte A devrait recevoir le message. Lambda continue d'interroger la file d'attente pour obtenir des mises à jour. Lorsqu'il y a un nouveau message, Lambda invoque votre fonction avec ces nouvelles données d'événement de la file d'attente. Votre fonction s'exécute et crée des journaux sur Amazon CloudWatch. Vous pouvez afficher les journaux dans la console CloudWatch .

Nettoyage de vos ressources

Vous pouvez maintenant supprimer les ressources que vous avez créées pour ce didacticiel, sauf si vous souhaitez les conserver. En supprimant AWS les ressources que vous n'utilisez plus, vous évitez des frais inutiles pour votre Compte AWS.

Dans le compte A, nettoyez votre rôle d'exécution et votre fonction d'événement Lambda.

Pour supprimer le rôle d'exécution

1. Ouvrez la page Roles (Rôles) de la console IAM.
2. Sélectionnez le rôle d'exécution que vous avez créé.
3. Sélectionnez Supprimer.
4. Saisissez le nom du rôle dans le champ de saisie de texte et choisissez Delete (Supprimer).

Pour supprimer la fonction d'événement Lambda

1. Ouvrez la page Event Functions de la console Lambda.
2. Sélectionnez la fonction d'événement que vous avez créée.
3. Sélectionnez Actions, Supprimer.
4. Saisissez **`confirm`** dans la zone de saisie de texte et choisissez Delete (Supprimer).

DansCompte B, nettoyez la file d’attente Amazon SQS.

Pour supprimer la file d’attente Amazon SQS

1. Connectez-vous à la console Amazon SQS Console de gestion AWS et ouvrez-la à l'adresse. https://console.aws.amazon.com/sqs/
2. Sélectionnez la file d’attente que vous avez créée.
3. Sélectionnez Supprimer.
4. Saisissez **`confirm`** dans le champ de saisie de texte.
5. Sélectionnez Supprimer.

Orchestration des fonctions d'événements Lambda avec Step Functions

AWS Step Functions fournit une orchestration visuelle du flux de travail pour coordonner les fonctions d'événement Lambda avec AWS d'autres services. Avec des intégrations natives à plus de 220 AWS services et une infrastructure entièrement gérée et ne nécessitant aucune maintenance, Step Functions est idéal lorsque vous avez besoin d'une conception visuelle de flux de travail et d'intégrations de services entièrement gérées.

Pour l'orchestration à l'aide de langages de programmation standard au sein de Lambda, où la logique du flux de travail côtoie la logique métier, pensez aux fonctions durables de Lambda. Pour vous aider à choisir entre ces options, consultez Durable functions ou Step Functions.

Par exemple, le traitement d’une commande peut nécessiter la validation des détails de la commande, la vérification des niveaux de stock, le traitement du paiement et la génération d’une facture. Écrivez des fonctions d'événement Lambda distinctes pour chaque tâche et utilisez Step Functions pour gérer le flux de travail. Step Functions coordonne le flux de données entre vos fonctions et gère les erreurs à chaque étape. Cette séparation facilite la visualisation, la modification et la maintenance de vos flux de travail à mesure qu’ils se complexifient.

Quand utiliser Step Functions avec Lambda

Les scénarios suivants sont de bons exemples de situations dans lesquelles Step Functions convient particulièrement bien à l'orchestration d' Lambda-based applications.

- Traitement séquentiel
- Gestion des erreurs complexes
- Flux de travail conditionnels et approbations humaines
- Traitement parallèle

Traitement séquentiel

Le traitement séquentiel se produit lorsqu’une tâche doit être terminée avant que la suivante puisse commencer. Par exemple, dans un système de traitement des commandes, le traitement des paiements ne peut pas commencer tant que la validation de la commande n’est pas terminée, et la génération des factures doit attendre la confirmation du paiement. Écrivez des fonctions d'événement Lambda distinctes pour chaque tâche et utilisez Step Functions pour gérer la séquence et le flux de données entre les fonctions.

Anti-pattern exemple

Une seule fonction d'événement Lambda gère l'ensemble du flux de travail de traitement des commandes en :

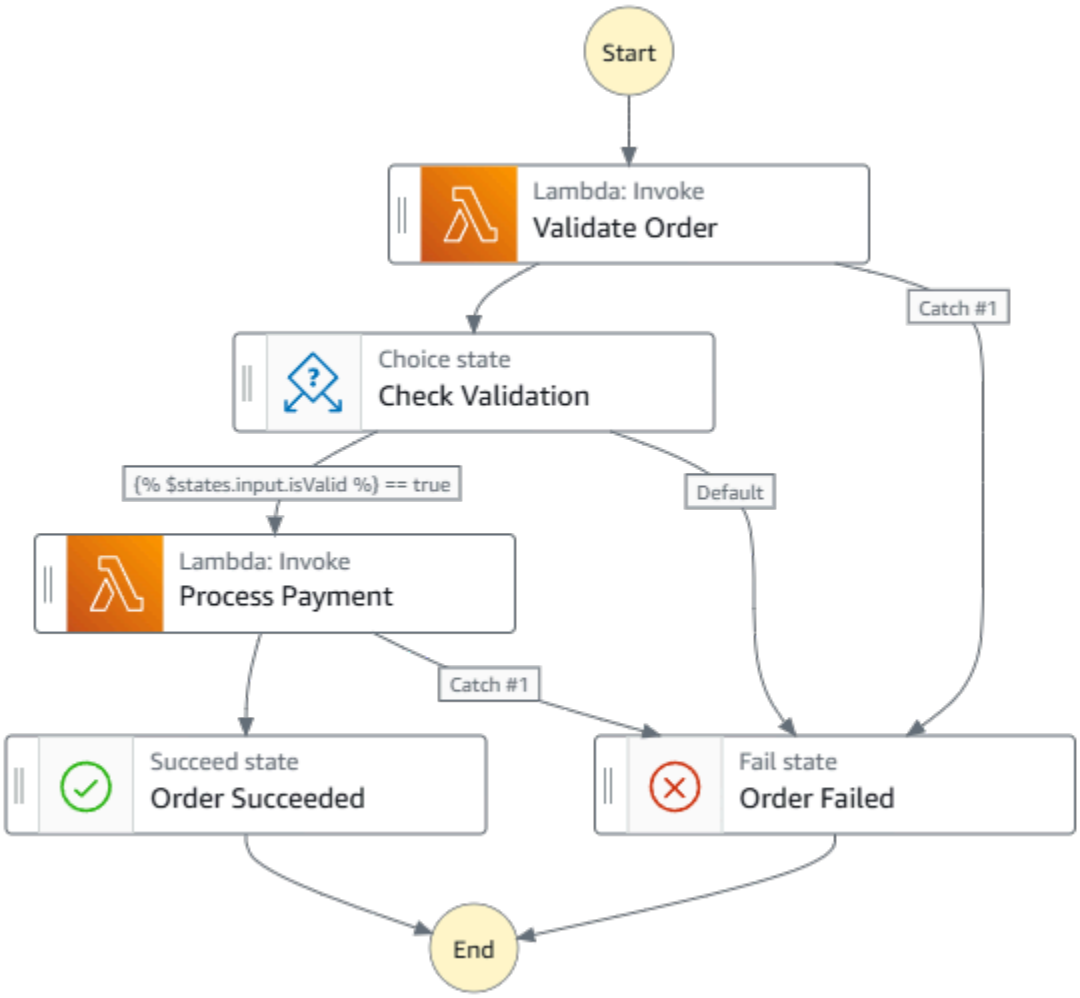
- Invocation d'autres fonctions d'événement Lambda en séquence
- Analysant et validant les réponses de chaque fonction
- Implémentant la gestion des erreurs et la logique de récupération
- Gérant le flux de données entre les fonctions

Approche recommandée

Utilisez deux fonctions d'événement Lambda : l'une pour valider la commande et l'autre pour traiter le paiement. Step Functions coordonne ces fonctions en :

- Exécutant les tâches dans le bon ordre
- Transmettant les données entre les fonctions
- Implémentant la gestion des erreurs à chaque étape
- Utilisant les états Choice pour s’assurer que seules les commandes valides sont réglées

Example graphique de flux de travail



> **Note**
>
> Code-first alternative : pour le traitement séquentiel avec point de contrôle et nouvelle tentative basés sur le code, voir les étapes relatives aux fonctions durables de Lambda.

Gestion des erreurs complexes

Bien que Lambda propose des fonctionnalités de nouvelle tentative pour les invocations asynchrones et les mappages des sources d'événements, Step Functions fournit une gestion des erreurs plus sophistiquée pour les flux de travail complexes. Vous pouvez configurer des nouvelles tentatives automatiques avec un backoff exponentiel et définir différentes politiques de tentatives pour différents types d'erreurs. Lorsque les tentatives sont épuisées, utilisez `Catch` pour rediriger les erreurs vers un

état de secours. Cela est particulièrement utile lorsque vous avez besoin d'une gestion des erreurs au niveau du flux de travail qui coordonne plusieurs fonctions et services.

Pour en savoir plus sur la gestion des erreurs liées à la fonction d'événement Lambda dans une machine à états, consultez la section Gestion des erreurs dans The AWS Step Functions Workshop.

Anti-pattern exemple

Une seule fonction d'événement Lambda gère tous les éléments suivants :

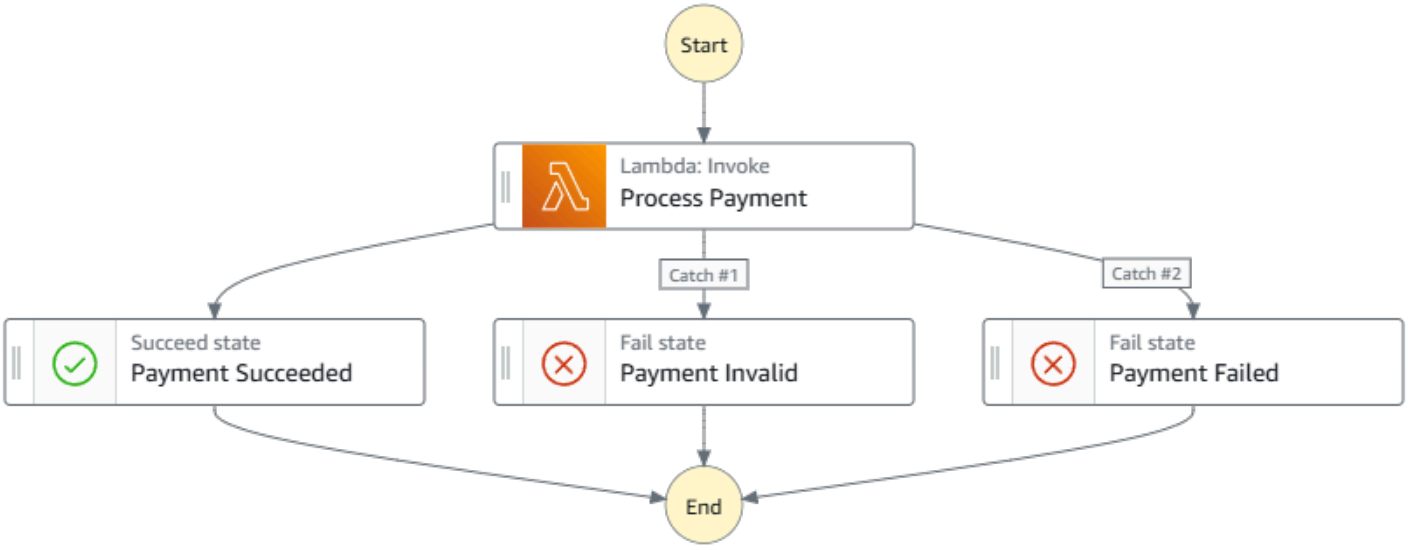
- Tentatives d'appel à un service de traitement des paiements
- Si le service de paiement n'est pas disponible, la fonction attend et essaie à nouveau ultérieurement.
- Implémente un backoff exponentiel personnalisé du temps d'attente
- Quand toutes les tentatives échouent, détecte l'erreur et choisit un autre flux

Approche recommandée

Utilisez une seule fonction d'événement Lambda axée uniquement sur le traitement des paiements. Step Functions gère la gestion des erreurs en :

- Réessayant automatiquement les tâches ayant échoué avec des périodes de backoff configurables
- Appliquant différentes politiques de nouvelle tentative en fonction des types d'erreur
- Acheminant différents types d'erreurs vers les états de secours appropriés
- Maintenant l'état et l'historique de gestion des erreurs

Example graphique de flux de travail



> **Note**
>
> Code-first alternative : Les fonctions durables permettent de gérer les erreurs d'essai avec des stratégies de nouvelle tentative configurables. Voir Gestion des erreurs dans les fonctions durables.

Flux de travail conditionnels et approbations humaines

Utilisez l'état Step Functions Choice pour acheminer les flux de travail en fonction du résultat de la fonction et du ForTaskToken suffixe d'attente pour suspendre les flux de travail pour des décisions humaines. Par exemple, pour traiter une demande d'augmentation de limite de crédit, utilisez une fonction d'événement Lambda pour évaluer les facteurs de risque. Utilisez ensuite Step Functions pour acheminer les demandes à haut risque vers une approbation manuelle et les demandes à faible risque vers une approbation automatique.

Pour déployer un exemple de flux de travail utilisant un modèle d'intégration de jeton de tâche de rappel, voir Rappel avec jeton de tâche dans The AWS Step Functions Workshop.

Anti-pattern exemple

Une seule fonction d'événement Lambda gère un flux de travail d'approbation complexe en :

- Implémentant une logique conditionnelle imbriquée pour évaluer les demandes de crédit

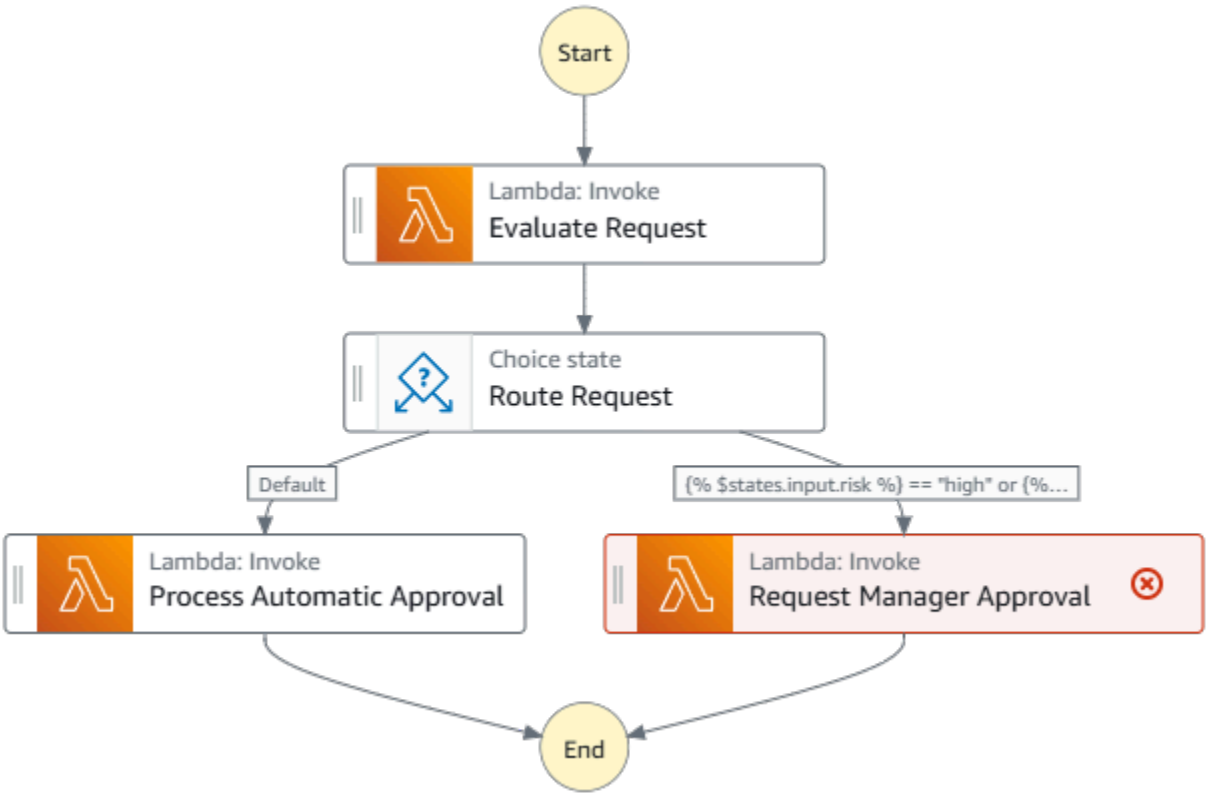
- Invoquant différentes fonctions d'approbation en fonction du montant des demandes
- Gérant plusieurs voies d'approbation et points de décision
- Suivant l'état des approbations en attente
- Implémentant une logique de délai d'expiration et de notification pour les approbations

Approche recommandée

Utilisez trois fonctions d'événement Lambda : une pour évaluer le risque de chaque demande, une pour approuver les demandes à faible risque et une pour acheminer les demandes à haut risque vers un responsable pour examen. Step Functions gère le flux de travail en :

- Utilisant les états Choice pour acheminer les demandes en fonction du montant et du niveau de risque
- Suspendant l'exécution en attendant l'approbation humaine
- Gérant les délais d'expiration pour les approbations en attente
- Fournissant une visibilité sur l'état actuel de chaque demande

Example graphique de flux de travail



> **Note**
>
> Code-first alternative : les fonctions durables prennent en charge les rappels pour les flux de travail axés sur l'humain. Voir Callbacks dans les fonctions durables.

Traitement parallèle

Step Functions propose trois méthodes pour gérer le traitement parallèle :

- L'état Parallel exécute simultanément plusieurs ramifications de votre flux de travail. Utilisez-le lorsque vous devez exécuter différentes fonctions en parallèle, comme la génération de vignettes lors de l'extraction des métadonnées des images.
- L'état Inline Map traite des tableaux de données avec jusqu'à 40 itérations simultanées. Utilisez-le pour les jeux de données de petite ou moyenne taille dans lesquels vous devez effectuer la même opération sur chaque élément.

- L'état Distributed Map gère un traitement parallèle à grande échelle avec jusqu'à 10 000 exécutions simultanées, prenant en charge à la fois les tableaux JSON et les sources de données Amazon Simple Storage Service (Amazon S3). Utilisez-le lorsque vous traitez de grands jeux de données ou lorsque vous avez besoin d'une plus grande simultanéité.

Anti-pattern exemple

Une seule fonction d'événement Lambda tente de gérer le traitement parallèle en :

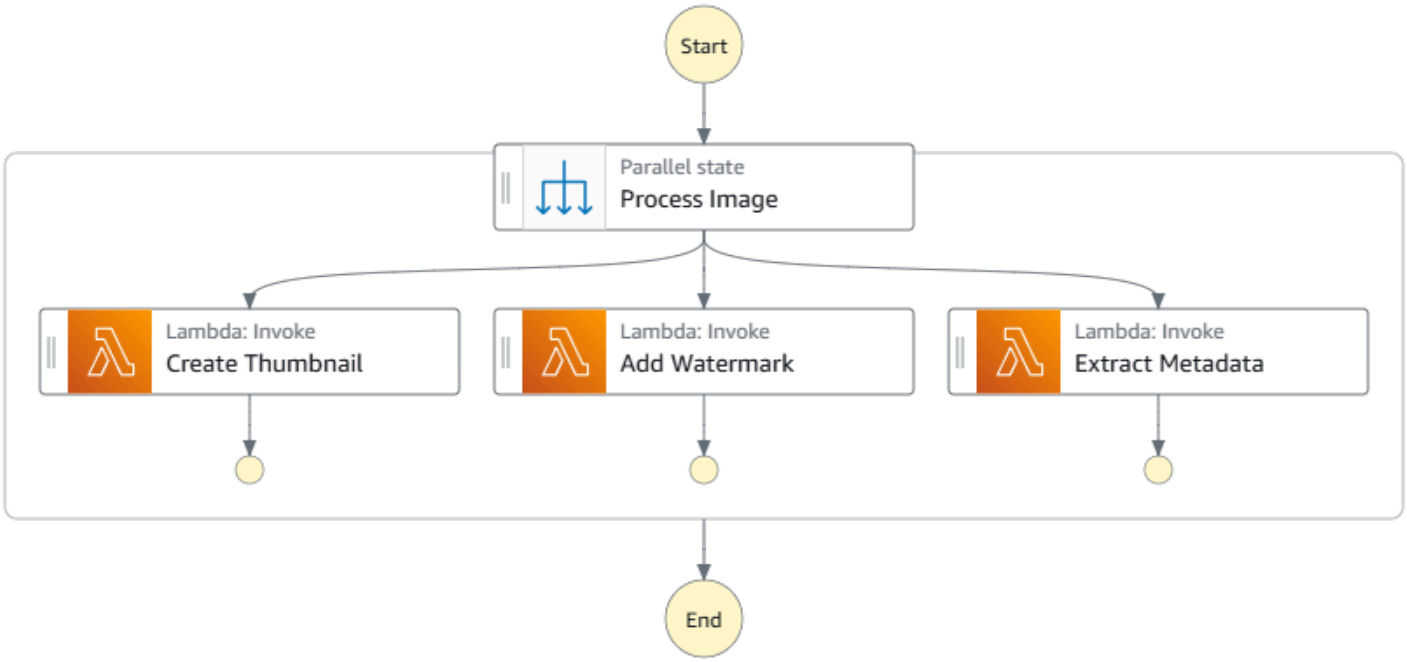
- Invoquant simultanément plusieurs fonctions de traitement d'image
- Implémentant une logique d'exécution parallèle personnalisée
- Gérant les délais d'attente et les erreurs pour chaque tâche parallèle
- Collectant et agrégeant les résultats de toutes les fonctions

Approche recommandée

Utilisez trois fonctions d'événement Lambda : une pour créer une image miniature, une pour ajouter un filigrane et une pour extraire les métadonnées. Step Functions gère ces fonctions en :

- Exécutant simultanément toutes les fonctions à l'aide de l'état Parallel
- Collectant les résultats de chaque fonction dans un tableau ordonné
- Gérant les délais d'expiration et les erreurs dans toutes les exécutions parallèles
- Continuant uniquement lorsque toutes les ramifications parallèles sont terminées

Example graphique de flux de travail



> **Note**
>
> Code-first alternative : fonctions `parallel()` et `map()` opérations durables. Voir Exécution parallèle.

Quand ne pas utiliser Step Functions avec Lambda

Toutes les Lambda-based applications ne bénéficient pas de l'utilisation de Step Functions. Envisagez ces scénarios lorsque vous choisissez l'architecture de votre application.

- Applications simples
- Traitement de données complexes
- CPU-intensive charges de travail

Applications simples

> **Note**
>
> Pour les flux de travail qui ne nécessitent pas de conception visuelle ou d'intégrations de services étendues, les fonctions durables de Lambda peuvent constituer une alternative plus simple qui permet de conserver la logique du flux de travail dans le code de Lambda.

Pour les applications qui ne nécessitent pas d'orchestration complexe, l'utilisation de Step Functions peut ajouter une complexité inutile. Par exemple, si vous traitez simplement des messages provenant d'une file d'attente Amazon SQS ou si vous répondez à EventBridge des événements Amazon, vous pouvez configurer ces services pour appeler directement vos fonctions d'événement Lambda. De même, si votre application ne comprend qu'une ou deux fonctions d'événement Lambda avec une gestion simple des erreurs, l'invocation directe de Lambda ou les architectures pilotées par les événements peuvent être plus simples à déployer et à gérer.

Traitement de données complexes

Vous pouvez utiliser l'état de la carte distribuée Step Functions pour traiter simultanément de grands ensembles de données Amazon S3 avec Lambda Event Functions. Cela est efficace pour de nombreuses charges de travail parallèles à grande échelle, notamment pour le traitement de données semi-structurées, comme des fichiers JSON ou CSV. Toutefois, pour des transformations de données plus complexes ou l'analytique avancée, envisagez les alternatives suivantes :

- Pipelines de transformation des données : AWS Glue à utiliser pour les tâches ETL qui traitent des données structurées ou semi-structurées provenant de sources multiples. AWS Glue est particulièrement utile lorsque vous avez besoin de fonctionnalités intégrées de gestion de schémas et de catalogues de données.
- Analytique des données : utilisez Amazon EMR pour l'analytique des données à l'échelle du pétaoctet, en particulier lorsque vous avez besoin d'outils de l'écosystème Apache Hadoop ou pour des charges de travail de machine learning qui dépassent les limites de mémoire de Lambda.

CPU-intensive charges de travail

Step Functions peut orchestrer CPU-intensive des tâches, mais les fonctions d'événement Lambda peuvent ne pas être adaptées à ces charges de travail en raison de leurs ressources CPU limitées.

Pour les opérations nécessitant des calculs intensifs au sein de vos flux de travail, envisagez les alternatives suivantes :

- Orchestration de conteneurs : utilisez Step Functions pour gérer les tâches Amazon Elastic Container Service (Amazon ECS) afin d'obtenir des ressources de calcul plus cohérentes et faciles à mettre à l'échelle.
- Traitement par lots : AWS Batch intégrez-le à Step Functions pour gérer les tâches par lots gourmandes en ressources informatiques qui nécessitent une utilisation soutenue du processeur.

Invoquer une fonction d'événement Lambda avec des événements par lots Amazon S3

Vous pouvez utiliser les opérations par lots Amazon S3 pour appeler une fonction d'événement Lambda sur un grand nombre d'objets Amazon S3. Amazon S3 effectue le suivi de la progression des opérations par lot, envoie des notifications et stocke un rapport d'achèvement indiquant le statut de chaque action.

Pour exécuter une opération par lot, vous créez une tâche d'opérations par lot Amazon S3. Lorsque vous créez le travail, vous fournissez un manifeste (la liste des objets) et configurez l'action à effectuer sur ces objets.

Lorsque le traitement par lots démarre, Amazon S3 invoque la fonction d'événement Lambda de manière synchrone pour chaque objet du manifeste. Le paramètre d'événement inclut les noms du compartiment et de l'objet.

L'exemple suivant montre l'événement qu'Amazon S3 envoie à la fonction d'événement Lambda pour un objet nommé customer Image1.jpg dans le compartiment amzn-s3-demo-bucket.

ExampleÉvénement de demande de lot Amazon S3

```
{
"invocationSchemaVersion": "1.0",
    "invocationId": "YXNkbGZqYWRmaiBhc2RmdW9hZHNmZGpmaGFzbGtkaGZza2RmaAo",
    "job": {
        "id": "f3cc4f60-61f6-4a2b-8a21-d07600c373ce"
    },
    "tasks": [
        {
            "taskId": "dGFza2lkZ29lc2hlcmUK",
            "s3Key": "customerImage1.jpg",
            "s3VersionId": "1",
            "s3BucketArn": "arn:aws:s3:::amzn-s3-demo-bucket"
        }
    ]
}
```

Votre fonction d'événement Lambda doit renvoyer un objet JSON avec les champs indiqués dans l'exemple suivant. Vous pouvez copier `invocationId` et `taskId` à partir du paramètre

d'événement. Vous pouvez renvoyer une chaîne dans `resultString`. Amazon S3 enregistre les valeurs `resultString` dans le rapport de fin de tâche.

Example Réponse à la demande de lot Amazon S3

```
{
  "invocationSchemaVersion": "1.0",
  "treatMissingKeysAs" : "PermanentFailure",
  "invocationId" : "YXNkbGZqYWRmaiBhc2RmdW9hZHNmZGpmaGFzbGtkaGZza2RmaAo",
  "results": [
    {
      "taskId": "dGFza2lkZ29lc2hlcmUK",
      "resultCode": "Succeeded",
      "resultString": "[\"Alice\", \"Bob\"]"
    }
  ]
}
```

Invocation de fonctions d'événement Lambda à partir d'opérations par lots Amazon S3

Vous pouvez appeler la fonction d'événement Lambda avec un ARN de fonction qualifié ou non qualifié. Si vous souhaitez utiliser la même version de fonction pour l'ensemble du travail par lot, configurez une version de fonction spécifique dans le paramètre `FunctionARN` lorsque vous créez votre travail. Si vous configurez un alias ou le qualificateur $LATEST, le travail par lot commence immédiatement à appeler la nouvelle version de la fonction si l'alias ou $LATEST est mis à jour pendant l'exécution du travail.

Notez que vous ne pouvez pas réutiliser une fonction Amazon S3 basée sur un événement existante pour des opérations par lot. Cela est dû au fait que l'opération par lots Amazon S3 transmet un paramètre d'événement différent à la fonction d'événement Lambda et attend un message de retour avec une structure JSON spécifique.

Dans la politique basée sur les ressources que vous créez pour la tâche par lots Amazon S3, assurez-vous que vous avez défini l'autorisation pour que la tâche appelle votre fonction d'événement Lambda.

Dans le rôle d'exécution pour la fonction, définissez une stratégie d'approbation pour qu'Amazon S3 endosse ce rôle lors de l'exécution de votre fonction.

Si votre fonction utilise le AWS SDK pour gérer les ressources Amazon S3, vous devez ajouter des autorisations Amazon S3 dans le rôle d'exécution.

Lorsque le travail s'exécute, Amazon S3 démarre plusieurs instances de fonction pour traiter les objets Amazon S3 en parallèle, jusqu'à la limite de simultanéité de la fonction. Amazon S3 limite la montée en puissance initiale des instances afin d'éviter des surcoûts pour les tâches de plus petite taille.

Si la fonction d'événement Lambda renvoie un code de `TemporaryFailure` réponse, Amazon S3 tente à nouveau l'opération.

Pour plus d'informations les opérations par lot Amazon S3, consultez Exécution d'opérations par lot dans le Manuel du développeur Amazon S3.

Pour un exemple d'utilisation d'une fonction d'événement Lambda dans les opérations par lots Amazon S3, consultez Invoking a Lambda function from Amazon S3 batch operations dans le manuel Amazon S3 Developer Guide.

Invocation des fonctions d'événement Lambda avec les notifications Amazon SNS

Vous pouvez utiliser une fonction d'événement Lambda pour traiter les notifications Amazon Simple Notification Service (Amazon SNS). Amazon SNS prend en charge les fonctions d'événement Lambda en tant que cible pour les messages envoyés à un sujet. Vous pouvez abonner votre fonction à des rubriques du même compte ou d'autres comptes AWS . Pour voir une procédure, consultez the section called "didacticiel".

Lambda prend en charge les déclencheurs SNS pour les rubriques SNS standard uniquement. Les rubriques FIFO ne sont pas prises en charge.

Lambda traite les messages SNS de manière asynchrone en les mettant en file d'attente et en gérant les nouvelles tentatives. Si Amazon SNS ne peut pas atteindre Lambda ou si le message est rejeté, Amazon SNS effectue de nouvelles tentatives à intervalles croissants pendant plusieurs heures. Pour plus de détails, consultes Fiabilité dans le FAQ sur Amazon SNS.

> **Warning**
>
> Les invocations asynchrones traitent chaque événement au moins une fois, et le traitement des enregistrements peut être dupliqué. Pour éviter les problèmes potentiels liés à des événements dupliqués, nous vous recommandons vivement de rendre votre code de fonction idempotent. Pour en savoir plus, consultez Comment rendre ma fonction Lambda idempotente dans le Knowledge Center. AWS

Utilitaire d'impuissance de Powertools pour AWS Lambda

L'utilitaire idempotencience de Powertools for Lambda rend vos fonctions d'événement AWS Lambda idempotentes. Il est disponible pour Python TypeScript, Java et .NET. Pour plus d'informations, consultez l'utilitaire Idempotency dans la documentation Powertools for Lambda AWS (Python), l'utilitaire Idempotency dans la documentation Powertools for Lambda (), l'utilitaire Idempotency dans la TypeScript documentation Powertools for AWS Lambda (Java) et l'utilitaire Idempotency dans la documentation Powertools for AWS Lambda (.NET). AWS

Rubriques

- Ajout d'un déclencheur de rubrique Amazon SNS pour une fonction d'événement Lambda à l'aide de la console

- Ajout manuel d'un déclencheur de rubrique Amazon SNS pour une fonction d'événement Lambda
- Exemple de forme d’évènement SNS
- Tutoriel : Utilisation AWS Lambda avec Amazon Simple Notification Service

Ajout d'un déclencheur de rubrique Amazon SNS pour une fonction d'événement Lambda à l'aide de la console

Pour ajouter un sujet SNS comme déclencheur pour une fonction d'événement Lambda, le moyen le plus simple consiste à utiliser la console Lambda. Lorsque vous ajoutez le déclencheur via la console, Lambda configure automatiquement les autorisations et les abonnements nécessaires pour commencer à recevoir des événements provenant de la rubrique SNS.

Pour ajouter une rubrique SNS comme déclencheur pour une fonction d'événement Lambda (console)

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez le nom de la fonction pour laquelle vous souhaitez ajouter le déclencheur.
3. Choisissez Configuration, puis Déclencheurs.
4. Choisissez Add trigger (Ajouter déclencheur).
5. Sous Configuration du déclencheur, dans le menu déroulant, choisissez SNS.
6. Pour Rubrique SNS, choisissez la rubrique SNS à laquelle vous abonner.

Ajout manuel d'un déclencheur de rubrique Amazon SNS pour une fonction d'événement Lambda

Pour configurer manuellement un déclencheur SNS pour une fonction d'événement Lambda, vous devez suivre les étapes suivantes :

- Définir une stratégie basée sur les ressources pour votre fonction afin de permettre à SNS de l’invoquer.
- Abonnez votre fonction d'événement Lambda à la rubrique Amazon SNS.

> **Note**
>
> Si votre rubrique SNS et votre fonction d'événement Lambda se trouvent sur des comptes AWS différents, vous devez également accorder des autorisations supplémentaires pour

autoriser les abonnements entre comptes à la rubrique SNS. Pour plus d'informations, consultez Accorder une autorisation multicompte pour l'abonnement Amazon SNS.

Vous pouvez utiliser le AWS Command Line Interface (AWS CLI) pour effectuer ces deux étapes. Tout d'abord, pour définir une politique basée sur les ressources pour une fonction d'événement Lambda qui autorise les appels SNS, utilisez la commande suivante. AWS CLI Assurez-vous de remplacer la valeur de par le nom `--function-name` de votre fonction d'événement Lambda et la valeur de par l'ARN `--source-arn` de votre rubrique SNS.

```
aws lambda add-permission --function-name example-function \
    --source-arn arn:aws:sns:us-east-1:123456789012:sns-topic-for-lambda \
    --statement-id function-with-sns --action "lambda:InvokeFunction" \
    --principal sns.amazonaws.com
```

Pour abonner votre fonction à la rubrique SNS, utilisez la AWS CLI commande suivante. Remplacez la valeur de `--topic-arn` par l'ARN de votre rubrique SNS et la valeur de par l'ARN de votre fonction `--notification-endpoint` d'événement Lambda.

```
aws sns subscribe --protocol lambda \
    --region us-east-1 \
    --topic-arn arn:aws:sns:us-east-1:123456789012:sns-topic-for-lambda \
    --notification-endpoint arn:aws:lambda:us-east-1:123456789012:function:example-
function
```

Exemple de forme d'évènement SNS

Amazon SNS appelle votre fonction de façon asynchrone avec un événement contenant un message et des métadonnées.

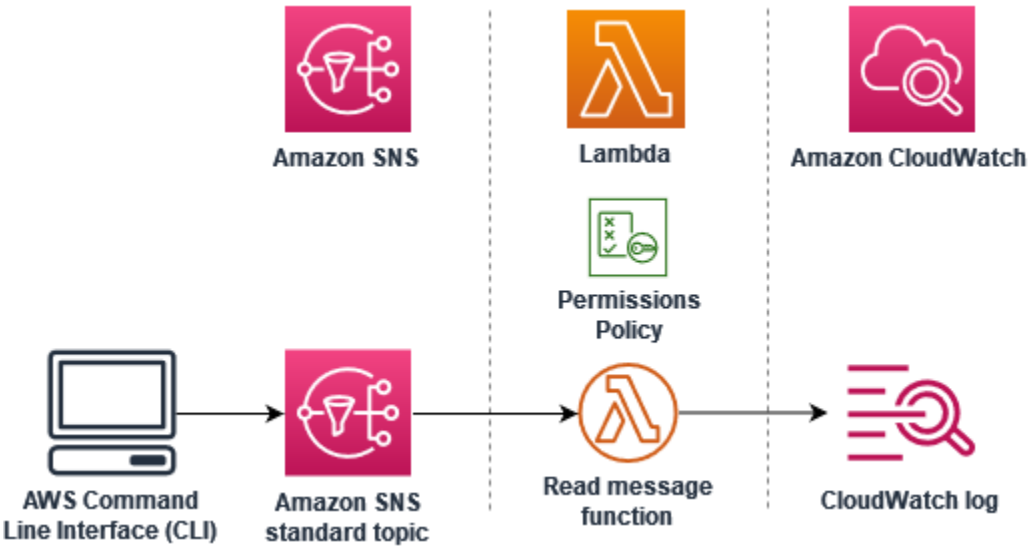
ExampleÉvénement de message Amazon SNS

```
{
  "Records": [
    {
      "EventVersion": "1.0",
      "EventSubscriptionArn": "arn:aws:sns:us-east-1:123456789012:sns-lambda:21be56ed-
a058-49f5-8c98-aedd2564c486",
      "EventSource": "aws:sns",
```

```
      "Sns": {
        "SignatureVersion": "1",
        "Timestamp": "2019-01-02T12:45:07.000Z",
        "Signature": "tcc6faL2yUC6dgZdmrwh1Y4cGa/ebXEkAi6RibDsvpi+tE/1+82j...65r==",
        "SigningCertURL": "https://sns.us-east-1.amazonaws.com/
SimpleNotificationService-ac565b8b1a6c5d002d285f9598aa1d9b.pem",
        "MessageId": "95df01b4-ee98-5cb9-9903-4c221d41eb5e",
        "Message": "Hello from SNS!",
        "MessageAttributes": {
          "Test": {
            "Type": "String",
            "Value": "TestString"
          },
          "TestBinary": {
            "Type": "Binary",
            "Value": "TestBinary"
          }
        },
        "Type": "Notification",
        "UnsubscribeUrl": "https://sns.us-east-1.amazonaws.com/?
Action=Unsubscribe&amp;SubscriptionArn=arn:aws:sns:us-east-1:123456789012:test-
lambda:21be56ed-a058-49f5-8c98-aedd2564c486",
        "TopicArn":"arn:aws:sns:us-east-1:123456789012:sns-lambda",
        "Subject": "TestInvoke"
      }
    }
  ]
}
```

Tutoriel : Utilisation AWS Lambda avec Amazon Simple Notification Service

Dans ce didacticiel, vous allez utiliser une fonction d'événement Lambda intégrée pour vous abonner Compte AWS à une rubrique Amazon Simple Notification Service (Amazon SNS) dans une rubrique distincte. Compte AWS Lorsque vous publiez des messages sur votre rubrique Amazon SNS, votre fonction d'événement Lambda lit le contenu du message et le transmet à Amazon Logs. CloudWatch Pour terminer ce didacticiel, vous devez utiliser le AWS Command Line Interface (AWS CLI).



Pour compléter ce tutoriel, effectuez les tâches suivantes :

- Dans le compte A, créez une rubrique Amazon SNS.
- Dans le compte B, créez une fonction d'événement Lambda qui lit les messages du sujet.
- Dans le compte B, créez un abonnement à la rubrique.
- Publiez des messages sur la rubrique Amazon SNS du compte A et vérifiez que la fonction d'événement Lambda du compte B les envoie dans Logs. CloudWatch

En suivant ces étapes, vous apprendrez à configurer une rubrique Amazon SNS pour appeler une fonction d'événement Lambda. Vous apprendrez également à créer une politique Gestion des identités et des accès AWS (IAM) qui autorise une ressource d'une autre Compte AWS à invoquer Lambda.

Dans le tutoriel, vous utilisez deux Comptes AWS différents. Les AWS CLI commandes illustrent cela en utilisant deux profils nommés appelés `accountA` et`accountB`, chacun étant configuré pour être utilisé avec un profil différent Compte AWS. Pour savoir comment configurer le AWS CLI pour utiliser différents profils, consultez la section Paramètres des fichiers de configuration et d'identification dans le guide de l'AWS Command Line Interface utilisateur de la version 2. Assurez-vous de configurer la même valeur par défaut Région AWS pour les deux profils.

Si les AWS CLI profils que vous créez pour les deux Comptes AWS utilisent des noms différents, ou si vous utilisez le profil par défaut et un profil nommé, modifiez les AWS CLI commandes dans les étapes suivantes selon vos besoins.

Conditions préalables

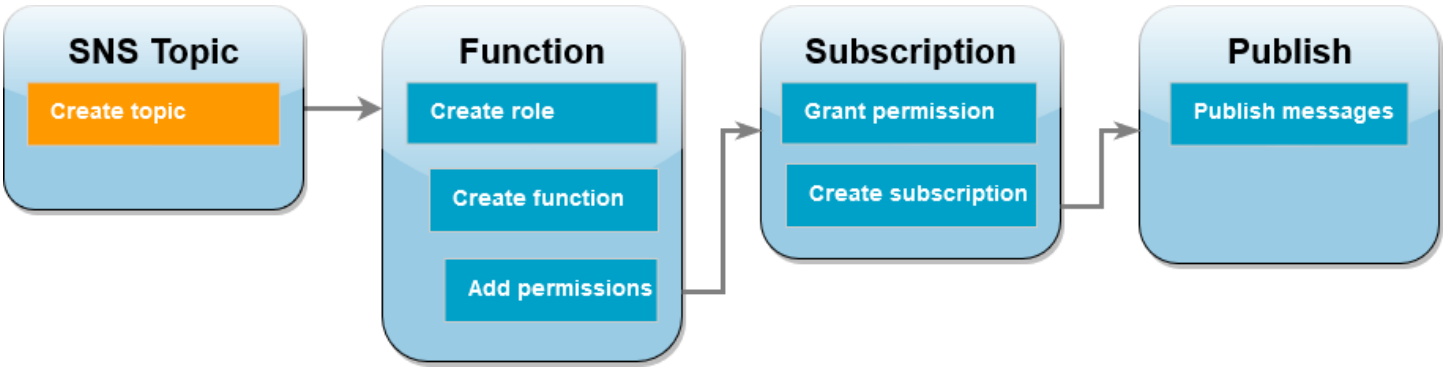
Installer la AWS Command Line Interface

Si vous ne l'avez pas encore installé AWS Command Line Interface, suivez les étapes décrites dans la section Installation ou mise à jour de la dernière version du AWS CLI pour l'installer.

Ce tutoriel nécessite un terminal de ligne de commande ou un shell pour exécuter les commandes. Sous Linux et macOS, utilisez votre gestionnaire de shell et de package préféré.

> **Note**
>
> Sous Windows, certaines commandes CLI Bash que vous utilisez couramment avec Lambda (par exemple `zip`) ne sont pas prises en charge par les terminaux intégrés du système d'exploitation. Pour obtenir une Windows-integrated version d'Ubuntu et de Bash, installez le sous-système Windows pour Linux.

Créer une rubrique Amazon SNS (compte A)



Pour créer la rubrique

- Dans le compte A, créez une rubrique standard Amazon SNS à l'aide de la commande suivante AWS CLI .

```
aws sns create-topic --name sns-topic-for-lambda --profile accountA
```

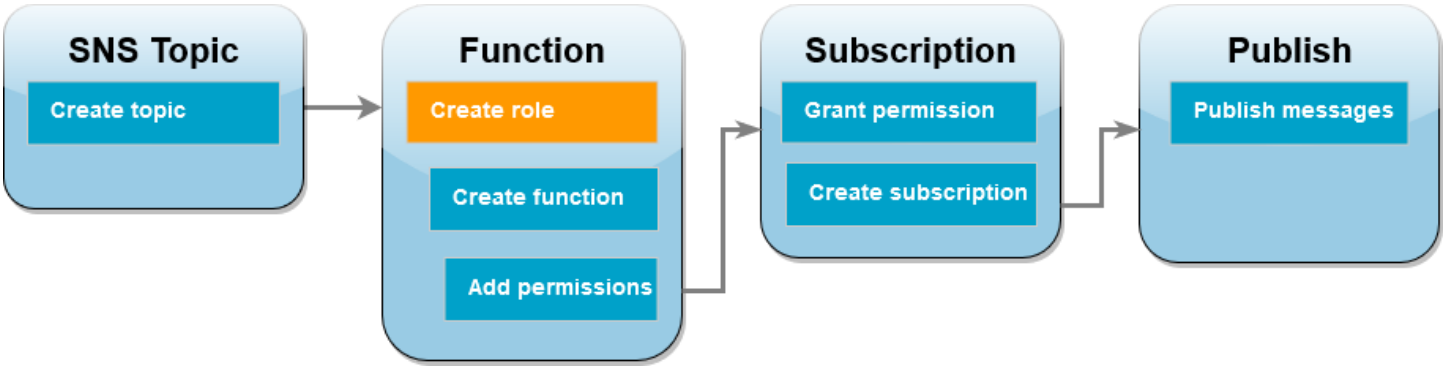
Vous devez visualiser des résultats similaires à ce qui suit.

```
{
    "TopicArn": "arn:aws:sns:us-west-2:123456789012:sns-topic-for-lambda"
```

```
}
```

Notez l'Amazon Resource Name (ARN) de votre rubrique. Vous en aurez besoin plus tard dans le didacticiel lorsque vous ajouterez des autorisations à votre fonction d'événement Lambda pour vous abonner au sujet.

Créer un rôle d'exécution de fonction (compte B)



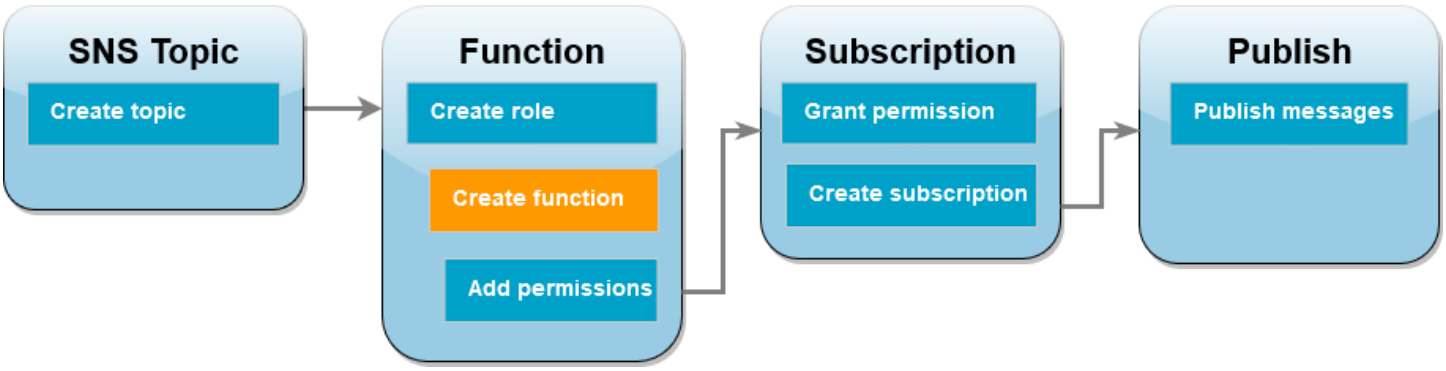
Un rôle d'exécution est un rôle IAM qui accorde à une fonction d'événement Lambda l'autorisation d' Services AWS accès et de ressources. Avant de créer votre fonction dans le compte B, vous devez créer un rôle qui donne à la fonction les autorisations de base pour écrire des journaux dans CloudWatch Logs. Nous ajouterons les autorisations de lecture de votre rubrique Amazon SNS lors d'une étape ultérieure.

Pour créer un rôle d'exécution

1. Dans le compte B, ouvrez la page des rôles dans la console IAM.
2. Choisissez Créer un rôle.
3. Pour Type d'entité de confiance, choisissez Service AWS .
4. Pour Cas d'utilisation, choisissez Lambda.
5. Choisissez Suivant.
6. Ajoutez une stratégie d'autorisations de base au rôle en procédant comme suit :
   a. Dans le champ de recherche Politiques d'autorisations, saisissez **`AWSLambdaBasicExecutionRole`**.
   b. Choisissez Suivant.
7. Finalisez la création du rôle en procédant comme suit :
   a. Sous Détails du rôle, saisissez **`lambda-sns-role`** pour Nom du rôle.

b. Choisissez Créer un rôle.

Création d'une fonction d'événement Lambda (compte B)



Créez une fonction d'événement Lambda qui traite vos messages Amazon SNS. Le code de fonction enregistre le contenu des messages de chaque enregistrement dans Amazon CloudWatch Logs.

Ce didacticiel utilise le runtime Node.js 24, mais nous avons également fourni des exemples de code dans d'autres langages d'exécution. Vous pouvez sélectionner l'onglet dans la zone suivante pour voir le code de l'exécution qui vous intéresse. Le JavaScript code que vous allez utiliser dans cette étape se trouve dans le premier exemple présenté dans l'JavaScriptonglet.

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement SNS avec Lambda à l'aide de .NET.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
using Amazon.Lambda.Core;
using Amazon.Lambda.SNSEvents;


// Assembly attribute to enable the Lambda function's JSON input to be converted
 into a .NET class.
```

```
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSeri

namespace SnsIntegration;

public class Function
{
    public async Task FunctionHandler(SNSEvent evnt, ILambdaContext context)
    {
        foreach (var record in evnt.Records)
        {
            await ProcessRecordAsync(record, context);
        }
        context.Logger.LogInformation("done");
    }

    private async Task ProcessRecordAsync(SNSEvent.SNSRecord record,
 ILambdaContext context)
    {
        try
        {
            context.Logger.LogInformation($"Processed record
 {record.Sns.Message}");

            // TODO: Do interesting work based on the new message
            await Task.CompletedTask;
        }
        catch (Exception e)
        {
            //You can use Dead Letter Queue to handle failures. By configuring a
 Lambda DLQ.
            context.Logger.LogError($"An error occurred");
            throw;
        }
    }
}
```

Go

Kit SDK pour Go V2

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement SNS avec Lambda à l'aide de Go.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package main

import (
 "context"
 "fmt"

 "github.com/aws/aws-lambda-go/events"
 "github.com/aws/aws-lambda-go/lambda"
)

func handler(ctx context.Context, snsEvent events.SNSEvent) {
 for _, record := range snsEvent.Records {
  processMessage(record)
 }
 fmt.Println("done")
}

func processMessage(record events.SNSEventRecord) {
 message := record.SNS.Message
 fmt.Printf("Processed message: %s\n", message)
 // TODO: Process your record here
}

func main() {
 lambda.Start(handler)
}
```

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement SNS avec Lambda à l'aide de Java.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package example;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.LambdaLogger;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.SNSEvent;
import com.amazonaws.services.lambda.runtime.events.SNSEvent.SNSRecord;


import java.util.Iterator;
import java.util.List;

public class SNSEventHandler implements RequestHandler<SNSEvent, Boolean> {
    LambdaLogger logger;

    @Override
    public Boolean handleRequest(SNSEvent event, Context context) {
        logger = context.getLogger();
        List<SNSRecord> records = event.getRecords();
        if (!records.isEmpty()) {
            Iterator<SNSRecord> recordsIter = records.iterator();
            while (recordsIter.hasNext()) {
                processRecord(recordsIter.next());
            }
        }
        return Boolean.TRUE;
    }

    public void processRecord(SNSRecord record) {
```

```
        try {
            String message = record.getSNS().getMessage();
            logger.log("message: " + message);
        } catch (Exception e) {
            throw new RuntimeException(e);
        }
    }

}
```

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement SNS avec JavaScript Lambda en utilisant.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
exports.handler = async (event, context) => {
  for (const record of event.Records) {
    await processMessageAsync(record);
  }
  console.info("done");
};

async function processMessageAsync(record) {
  try {
    const message = JSON.stringify(record.Sns.Message);
    console.log(`Processed message ${message}`);
    await Promise.resolve(1); //Placeholder for actual async work
  } catch (err) {
    console.error("An error occurred");
```

```
    throw err;
  }
}
```

Consommation d'un événement SNS avec TypeScript Lambda en utilisant.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import { SNSEvent, Context, SNSHandler, SNSEventRecord } from "aws-lambda";

export const functionHandler: SNSHandler = async (
  event: SNSEvent,
  context: Context
): Promise<void> => {
  for (const record of event.Records) {
    await processMessageAsync(record);
  }
  console.info("done");
};

async function processMessageAsync(record: SNSEventRecord): Promise<any> {
  try {
    const message: string = JSON.stringify(record.Sns.Message);
    console.log(`Processed message ${message}`);
    await Promise.resolve(1); //Placeholder for actual async work
  } catch (err) {
    console.error("An error occurred");
    throw err;
  }
}
```

PHP

Kit SDK pour PHP

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Utilisation d'un événement SNS avec Lambda à l'aide de PHP.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
<?php

/*
Since native PHP support for AWS Lambda is not available, we are utilizing Bref's
 PHP functions runtime for AWS Lambda.
For more information on Bref's PHP runtime for Lambda, refer to: https://bref.sh/
docs/runtimes/function

Another approach would be to create a custom runtime.
A practical example can be found here: https://aws.amazon.com/blogs/apn/aws-
lambda-custom-runtime-for-php-a-practical-example/
*/

// Additional composer packages may be required when using Bref or any other PHP
 functions runtime.
// require __DIR__ . '/vendor/autoload.php';

use Bref\Context\Context;
use Bref\Event\Sns\SnsEvent;
use Bref\Event\Sns\SnsHandler;

class Handler extends SnsHandler
{
    public function handleSns(SnsEvent $event, Context $context): void
    {
        foreach ($event->getRecords() as $record) {
            $message = $record->getMessage();

            // TODO: Implement your custom processing logic here
            // Any exception thrown will be logged and the invocation will be
 marked as failed

            echo "Processed Message: $message" . PHP_EOL;
        }
    }
}

return new Handler();
```

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Utilisation d'un événement SNS avec Lambda à l'aide de Python.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
def lambda_handler(event, context):
    for record in event['Records']:
        process_message(record)
    print("done")

def process_message(record):
    try:
        message = record['Sns']['Message']
        print(f"Processed message {message}")
        # TODO; Process your record here

    except Exception as e:
        print("An error occurred")
        raise e
```

Ruby

Kit SDK pour Ruby

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement SNS avec Lambda à l'aide de Ruby.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
def lambda_handler(event:, context:)
  event['Records'].map { |record| process_message(record) }
end

def process_message(record)
  message = record['Sns']['Message']
  puts("Processing message: #{message}")
rescue StandardError => e
  puts("Error processing message: #{e}")
  raise
end
```

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Utilisation d'un événement SNS avec Lambda à l'aide de Rust.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
use aws_lambda_events::event::sns::SnsEvent;
use aws_lambda_events::sns::SnsRecord;
use lambda_runtime::{run, service_fn, Error, LambdaEvent};
use tracing::info;

// Built with the following dependencies:
//  aws_lambda_events = { version = "0.10.0", default-features = false, features
 = ["sns"] }
//  lambda_runtime = "0.8.1"
//  tokio = { version = "1", features = ["macros"] }
```

```
//  tracing = { version = "0.1", features = ["log"] }
//  tracing-subscriber = { version = "0.3", default-features = false, features =
 ["fmt"] }

async fn function_handler(event: LambdaEvent<SnsEvent>) -> Result<(), Error> {
    for event in event.payload.records {
        process_record(&event)?;
    }

    Ok(())
}

fn process_record(record: &SnsRecord) -> Result<(), Error> {
    info!("Processing SNS Message: {}", record.sns.message);

    // Implement your record handling code here.

    Ok(())
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    tracing_subscriber::fmt()
        .with_max_level(tracing::Level::INFO)
        .with_target(false)
        .without_time()
        .init();

    run(service_fn(function_handler)).await
}
```

Pour créer la fonction d'événement

1. Créez un répertoire pour le projet, puis passez à ce répertoire.

```
mkdir sns-tutorial
cd sns-tutorial
```

2. Copiez l'exemple de JavaScript code dans un nouveau fichier nomméindex.js.
3. Créez un package de déploiement à l’aide de la commande zip suivante.

```
zip function.zip index.js
```

4. Exécutez la AWS CLI commande suivante pour créer votre fonction d'événement Lambda dans le compte B.

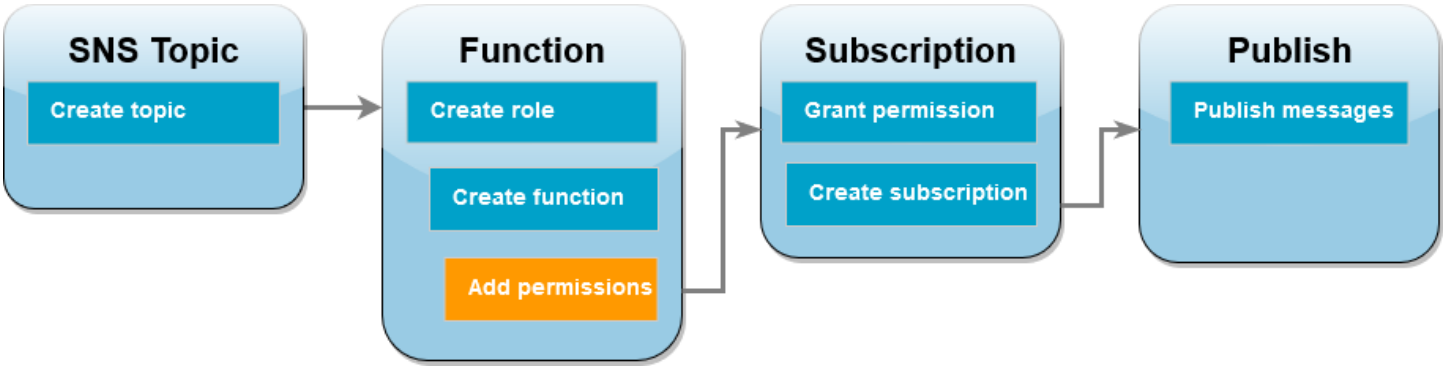
```
aws lambda create-function --function-name Function-With-SNS \
    --zip-file fileb://function.zip --handler index.handler --runtime nodejs24.x \
    --role arn:aws:iam::<AccountB_ID>:role/lambda-sns-role  \
    --timeout 60 --profile accountB
```

Vous devez visualiser des résultats similaires à ce qui suit.

```
{
    "FunctionName": "Function-With-SNS",
    "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:Function-With-
SNS",
    "Runtime": "nodejs24.x",
    "Role": "arn:aws:iam::123456789012:role/lambda_basic_role",
    "Handler": "index.handler",
    ...
    "RuntimeVersionConfig": {
        "RuntimeVersionArn": "arn:aws:lambda:us-
west-2::runtime:7d5f06b69c951da8a48b926ce280a9daf2e8bb1a74fc4a2672580c787d608206"
    }
}
```

5. Enregistrez l'Amazon Resource Name (ARN) de votre fonction. Vous en aurez besoin plus tard dans le didacticiel lorsque vous ajouterez des autorisations permettant à Amazon SNS d'appeler votre fonction.

Ajouter des autorisations à Event Function (compte B)



Pour qu'Amazon SNS puisse invoquer votre fonction, vous devez lui accorder une autorisation dans une instruction sur une stratégie basée sur les ressources. Vous ajoutez cette instruction à l'aide de la AWS CLI `add-permission` commande.

Pour autoriser Amazon SNS à invoquer votre fonction événementielle

- Dans le compte B, exécutez la AWS CLI commande suivante en utilisant l'ARN de votre rubrique Amazon SNS que vous avez enregistrée précédemment.

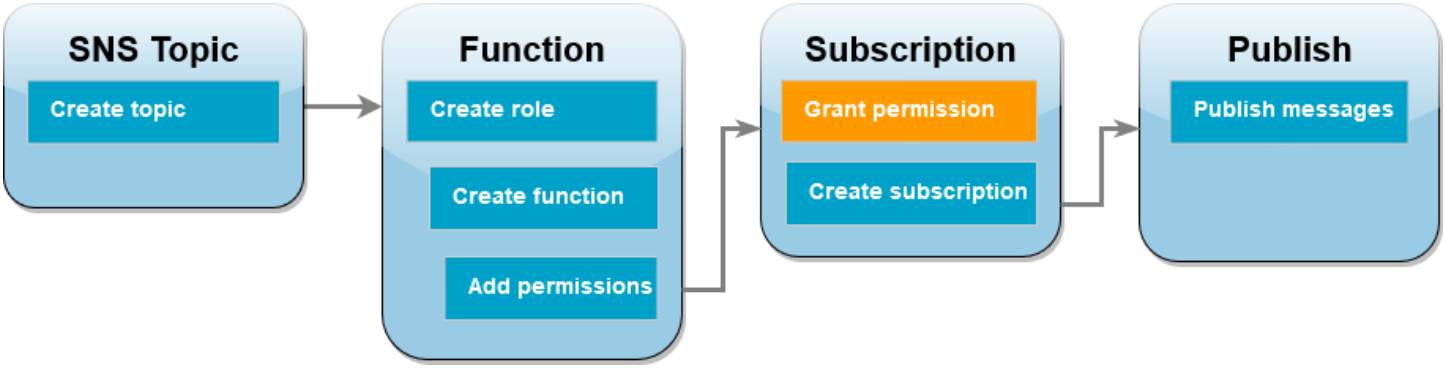
```
aws lambda add-permission --function-name Function-With-SNS \
    --source-arn arn:aws:sns:us-east-1:<AccountA_ID>:sns-topic-for-lambda \
    --statement-id function-with-sns --action "lambda:InvokeFunction" \
    --principal sns.amazonaws.com --profile accountB
```

  Vous devez visualiser des résultats similaires à ce qui suit.

```
{
    "Statement": "{\"Condition\":{\"ArnLike\":{\"AWS:SourceArn\":
      \"arn:aws:sns:us-east-1:<AccountA_ID>:sns-topic-for-lambda\"}},
      \"Action\":[\"lambda:InvokeFunction\"],
      \"Resource\":\"arn:aws:lambda:us-east-1:<AccountB_ID>:function:Function-With-
SNS\",
      \"Effect\":\"Allow\",\"Principal\":{\"Service\":\"sns.amazonaws.com\"},
      \"Sid\":\"function-with-sns\"}"
}
```

> **Note**
>
> Si le compte associé à la rubrique Amazon SNS est hébergé dans le cadre d'un opt-in Région AWS, vous devez spécifier la région dans le principal. Si vous travaillez par exemple avec une rubrique Amazon SNS dans la région Asie-Pacifique (Hong Kong), vous devez spécifier `sns.ap-east-1.amazonaws.com` au lieu de `sns.amazonaws.com` pour le principal.

Accorder une autorisation multicompte pour l'abonnement Amazon SNS (compte A)



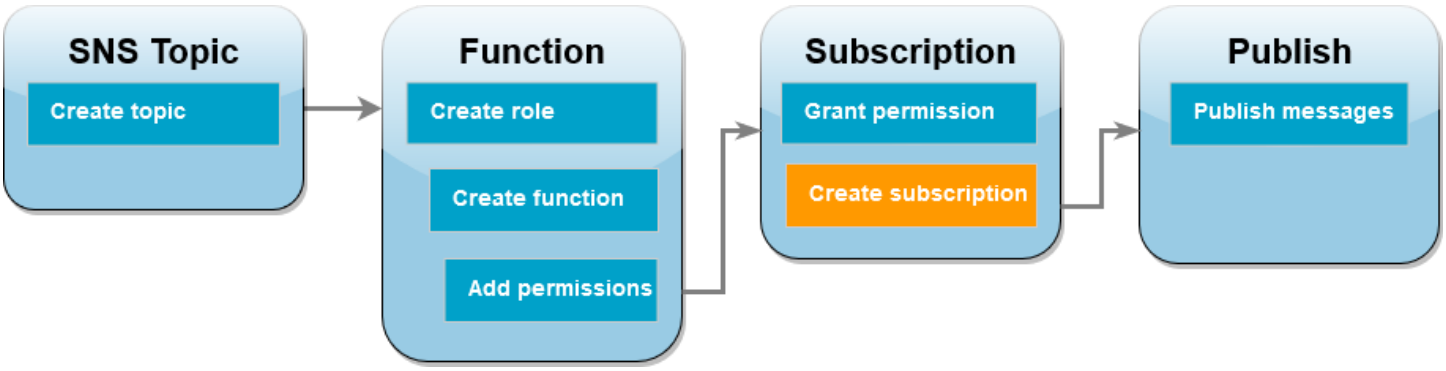
Pour que votre fonction d'événement Lambda sur le compte B puisse s'abonner à la rubrique Amazon SNS que vous avez créée dans le compte A, vous devez autoriser le compte B à s'abonner à votre sujet. Vous accordez cette autorisation à l'aide de la AWS CLI `add-permission` commande.

Pour accorder l'autorisation permettant au compte B de s'abonner à la rubrique

- Dans le compte A, exécutez la AWS CLI commande suivante. Utilisez l'ARN pour la rubrique Amazon SNS que vous avez enregistrée précédemment.

```
aws sns add-permission --label lambda-access --aws-account-id <AccountB_ID> \
    --topic-arn arn:aws:sns:us-east-1:<AccountA_ID>:sns-topic-for-lambda \
    --action-name Subscribe ListSubscriptionsByTopic --profile accountA
```

Créer un abonnement (compte B)



Dans le compte B, vous abonnez désormais votre fonction d'événement Lambda à la rubrique Amazon SNS que vous avez créée au début du didacticiel dans le compte A. Lorsqu'un message est envoyé à cette rubrique (**`sns-topic-for-lambda`**), Amazon SNS invoque votre fonction d'événement Lambda dans le compte B. **`Function-With-SNS`**

Pour créer un abonnement

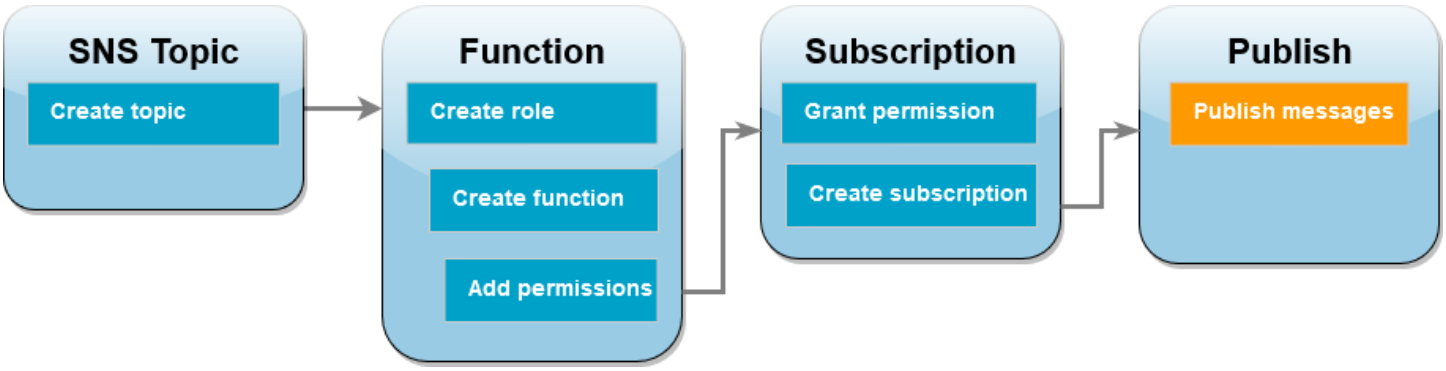
- Dans le compte B, exécutez la AWS CLI commande suivante. Utilisez la région par défaut dans laquelle vous avez créé votre sujet, ainsi que les ARN de votre sujet et de la fonction d'événement Lambda.

```
aws sns subscribe --protocol lambda \
    --region us-east-1 \
    --topic-arn arn:aws:sns:us-east-1:<AccountA_ID>:sns-topic-for-lambda \
    --notification-endpoint arn:aws:lambda:us-
east-1:<AccountB_ID>:function:Function-With-SNS \
    --profile accountB
```

Vous devez visualiser des résultats similaires à ce qui suit.

```
{
    "SubscriptionArn": "arn:aws:sns:us-east-1:<AccountA_ID>:sns-topic-for-
lambda:5d906xxxx-7c8x-45dx-a9dx-0484e31c98xx"
}
```

Publier des messages sur la rubrique (compte A et compte B)



Maintenant que votre fonction d'événement Lambda dans le compte B est abonnée à votre rubrique Amazon SNS dans le compte A, il est temps de tester votre configuration en publiant des messages sur votre sujet. Pour confirmer qu'Amazon SNS a invoqué votre fonction d'événement Lambda, vous utilisez les CloudWatch journaux pour afficher le résultat de votre fonction.

Pour publier un message sur votre sujet et consulter le résultat de votre fonction d'événement

1. Saisissez `Hello World` dans un fichier texte et enregistrez-le sous `message.txt`.

2. À partir du répertoire dans lequel vous avez enregistré votre fichier texte, exécutez la AWS CLI commande suivante dans le compte A. Utilisez l'ARN pour votre propre sujet.

```
aws sns publish --message file://message.txt --subject Test \
    --topic-arn arn:aws:sns:us-east-1:<AccountA_ID>:sns-topic-for-lambda \
    --profile accountA
```

   Cela renvoie un ID de message avec un identifiant unique, indiquant qu'Amazon SNS a accepté le message. Amazon SNS tente ensuite de transmettre le message aux abonnés du sujet. Pour vérifier qu'Amazon SNS a invoqué votre fonction d'événement Lambda, utilisez les CloudWatch journaux pour afficher le résultat de votre fonction :

3. Dans le compte B, ouvrez la page Log groups de la CloudWatch console Amazon.
4. Choisissez le groupe de journaux de votre fonction (`/aws/lambda/Function-With-SNS`).
5. Choisissez le flux de journaux le plus récent.
6. Si votre fonction a été correctement invoquée, vous verrez un résultat similaire au suivant indiquant le contenu du message que vous avez publié dans votre sujet.

```
2023-07-31T21:42:51.250Z c1cba6b8-ade9-4380-aa32-d1a225da0e48 INFO Processed
 message Hello World
2023-07-31T21:42:51.250Z c1cba6b8-ade9-4380-aa32-d1a225da0e48 INFO done
```

Nettoyage de vos ressources

Vous pouvez maintenant supprimer les ressources que vous avez créées pour ce didacticiel, sauf si vous souhaitez les conserver. En supprimant AWS les ressources que vous n'utilisez plus, vous évitez des frais inutiles pour votre Compte AWS.

Dans le compte A, nettoyez votre rubrique Amazon SNS.

Pour supprimer la rubrique Amazon SNS

1. Ouvrez la page Topics (Rubriques) de la console Amazon SNS.
2. Sélectionnez la rubrique que vous avez créée.
3. Choisissez Supprimer.
4. Saisissez **`delete me`** dans le champ de saisie de texte.
5. Sélectionnez Supprimer.

Dans le compte B, nettoyez votre rôle d'exécution, votre fonction d'événement Lambda et votre abonnement Amazon SNS.

Pour supprimer le rôle d'exécution

1. Ouvrez la page Roles (Rôles) de la console IAM.
2. Sélectionnez le rôle d'exécution que vous avez créé.
3. Sélectionnez Supprimer.
4. Saisissez le nom du rôle dans le champ de saisie de texte et choisissez Delete (Supprimer).

Pour supprimer la fonction d'événement Lambda

1. Ouvrez la page Event Functions de la console Lambda.
2. Sélectionnez la fonction d'événement que vous avez créée.
3. Sélectionnez Actions, Supprimer.
4. Saisissez **`confirm`** dans la zone de saisie de texte et choisissez Delete (Supprimer).

Pour supprimer l'abonnement Amazon SNS

1. Ouvrez la page Subscriptions (Abonnements) de la console Amazon SNS.
2. Sélectionnez l'abonnement que vous avez créé.
3. Choisissez Delete (Supprimer), Delete (Supprimer).

Fonctions durables Lambda

Avec AWS Lambda des fonctions durables, vous pouvez créer des applications résilientes en plusieurs étapes et des flux de travail d'IA qui peuvent être exécutés pendant une période allant jusqu'à un an tout en maintenant des progrès fiables malgré les interruptions. Lorsqu'une fonction durable est exécutée, ce cycle de vie complet est appelé « exécution durable », qui utilise des points de contrôle pour suivre la progression et récupérer automatiquement les défaillances par le biais d'une relecture, en réexécutant depuis le début tout en sautant le travail terminé.

Dans chaque fonction, vous utilisez des opérations durables comme éléments de base fondamentaux. Les étapes exécutent une logique métier avec des nouvelles tentatives intégrées et un suivi de la progression, tandis que les temps d'attente interrompent l'exécution sans entraîner

de frais de calcul, ce qui les rend idéales pour les processus de longue durée tels que les flux de travail interconnectés ou les interrogations de dépendances externes. Qu'il s'agisse de traiter des commandes, de coordonner des microservices ou d'orchestrer des applications d'IA agentiques, les fonctions durables maintiennent l'état automatiquement et se rétablissent en cas de panne pendant que vous écrivez du code dans des langages de programmation familiers.

> **Note**
>
> Ce guide couvre les sujets relatifs aux services Lambda tels que le déploiement, la configuration, les autorisations, l'invocation, la surveillance et les quotas. Pour obtenir des informations de référence sur la programmation du SDK, des didacticiels de démarrage rapide et des guides spécifiques à chaque langue, consultez le AWS Guide du développeur du SDK Durable Execution.

Principaux avantages

Écrivez du code résilient naturellement : Avec des structures de programmation familières, vous écrivez du code qui gère automatiquement les échecs. Built-in les points de contrôle, les nouvelles tentatives transparentes et la restauration automatique garantissent que votre logique métier reste claire et précise.

Payez uniquement pour ce que vous utilisez : Pendant les opérations d'attente, votre fonction est suspendue sans frais de calcul. Pour les flux de travail de longue durée qui attendent des heures ou des jours, vous ne payez que pour le temps de traitement réel, et non pour les temps d'attente inactifs.

Simplicité opérationnelle : Avec le modèle sans serveur de Lambda, vous bénéficiez d'une mise à l'échelle automatique, y compris une mise à l'échelle à zéro, sans gérer l'infrastructure. Les fonctions durables gèrent automatiquement la gestion de l'état, la logique des nouvelles tentatives et la reprise après panne, réduisant ainsi les frais opérationnels.

Quand utiliser des fonctions durables

Short-lived coordination : Coordonnez les paiements, les stocks et les expéditions entre plusieurs services grâce à une fonction d'annulation automatique en cas de panne. Traitez les commandes par le biais de la validation, de l'autorisation de paiement, de la répartition des stocks et de l'exécution avec garantie d'achèvement.

Traitez les paiements en toute confiance : Créez des flux de paiement résilients qui maintiennent l'état des transactions en cas d'échec et gèrent automatiquement les nouvelles tentatives. Coordonnez l'autorisation en plusieurs étapes, les contrôles antifraude et le règlement entre les fournisseurs de paiement avec une auditabilité complète à chaque étape.

Créez des flux de travail d'IA fiables : Créez des flux de travail d'IA en plusieurs étapes qui enchaînent les appels de modèles, intègrent le feedback humain et gèrent les tâches de longue durée de manière déterministe en cas de défaillance. Reprenez automatiquement après la suspension et ne payez que pour le temps d'exécution actif.

Orchestrez le traitement des commandes complexes : Coordonnez le traitement des commandes entre les systèmes d'inventaire, de paiement, d'expédition et de notification grâce à la résilience intégrée. Gérez automatiquement les défaillances partielles, préservez l'état de la commande malgré les interruptions et attendez efficacement les événements externes sans consommer de ressources de calcul.

Automatisez les flux de travail en plusieurs étapes : Créez des flux de travail fiables pour l'intégration des employés, l'approbation des prêts et les processus de conformité qui s'étendent sur des jours ou des semaines. Maintenez l'état du flux de travail en ce qui concerne les approbations humaines, les intégrations de systèmes et les tâches planifiées, tout en offrant une visibilité complète sur l'état et l'historique des processus.

Comparaison entre les fonctions durables et les fonctions Step

Les fonctions durables et Step Functions fournissent une orchestration du flux de travail avec une gestion automatique de l'état. Les principales différences résident dans leur mode d'exécution et dans la manière dont vous définissez les flux de travail :

- Fonctions durables : Exécuté dans Lambda, utilisation de langages de programmation standard, géré dans un environnement Lambda
- Fonctions de l'étape : Service autonome, DSL ou concepteur visuel basé sur des graphiques, entièrement géré sans maintenance

Les fonctions durables sont idéales pour le développement d'applications dans Lambda, où les flux de travail sont étroitement liés à la logique métier. Step Functions excelle dans l'orchestration des flux de travail dans AWS des services pour lesquels vous avez besoin d'une conception visuelle, d'intégrations natives à plus de 220 services et d'une infrastructure ne nécessitant aucune maintenance.

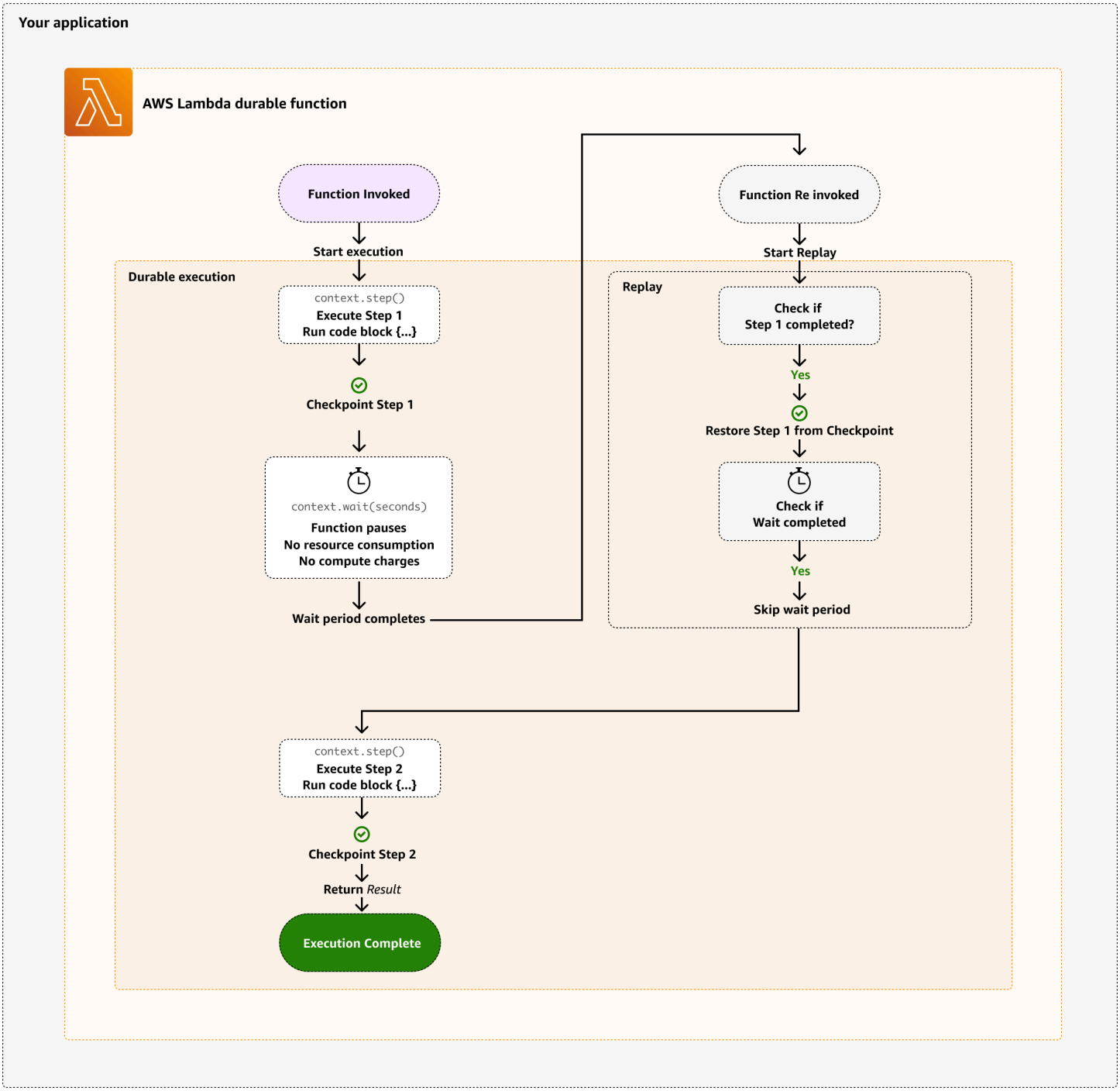
Pour une comparaison détaillée, voir Fonctions durables ou fonctions par étapes.

Comment ça marche

Sous le capot, les fonctions durables sont des fonctions Lambda classiques utilisant un checkpoint/replay mécanisme permettant de suivre les progrès et de soutenir les opérations de longue durée grâce à des points de suspension définis par l'utilisateur, communément appelés exécution durable. Une fois que votre fonction reprend après une pause ou une interruption, le système effectue une rediffusion. Pendant le replay, votre code s'exécute depuis le début mais ignore les points de contrôle terminés, en utilisant les résultats enregistrés au lieu de réexécuter les opérations terminées. Ce mécanisme de rediffusion garantit la cohérence tout en permettant des exécutions de longue durée.

Pour exploiter ce mécanisme de point de contrôle et de relecture dans vos applications, Lambda fournit un SDK d'exécution durable. Le SDK simplifie la gestion des points de contrôle et des rediffusions, en exposant de simples primitives appelées opérations durables que vous utilisez dans votre code. Le SDK est disponible pour JavaScript, TypeScript, Python, Java, Go et C# (.NET), s'intégrant parfaitement à votre flux de travail de développement Lambda existant.

Avec le SDK, vous encapsulez votre gestionnaire d'événements Lambda, qui fournit ensuite un DurableContext parallèlement à votre événement. Ce contexte vous donne accès à des opérations durables telles que les étapes et les attentes. Vous écrivez la logique de votre fonction sous la forme d'un code séquentiel normal, mais au lieu d'appeler directement les services, vous encapsulez ces appels par étapes pour des points de contrôle automatiques et des nouvelles tentatives. Lorsque vous devez suspendre l'exécution, vous ajoutez des temps d'attente qui interrompent votre fonction sans frais. Le SDK gère toute la complexité de la gestion des états et de la relecture en arrière-plan, afin que votre code reste propre et lisible.



Étapes suivantes

- AWS Guide du développeur du SDK Durable Execution — Référence du SDK, démarrages rapides, tests et guides linguistiques
- Commencez avec des fonctions durables
- Fonctions durables ou fonctions par étapes

- Surveillez et déboguez les fonctions durables
- Vérifiez la sécurité et les autorisations
- Chiffrement AWS Lambda données d'exécution durables
- Suivez les meilleures pratiques

Concepts de base

Le AWS Le SDK Durable Execution constitue la base de la création de fonctions durables, en fournissant les primitives dont vous avez besoin pour contrôler la progression des points, gérer les nouvelles tentatives et gérer le flux d'exécution. Le SDK est disponible pour Node.js (JavaScript et TypeScript), Python, Java, Go et C# (.NET). Pour obtenir une documentation complète sur le SDK, y compris des références d'API, des didacticiels de démarrage rapide et des guides spécifiques à une langue, consultez AWS Guide du développeur du SDK Durable Execution.

Exécution durable

UNE exécution durable représente le cycle de vie complet d'une fonction Lambda durable, en utilisant un point de contrôle et un mécanisme de relecture pour suivre la progression de la logique métier, suspendre l'exécution et récupérer en cas de défaillance. Lorsque les fonctions reprennent après une suspension ou des interruptions, les points de contrôle précédemment complétés sont rejoués et la fonction continue à s'exécuter.

Le cycle de vie peut inclure plusieurs appels d'une fonction Lambda pour terminer l'exécution, en particulier après une suspension ou une reprise après un échec. Cette approche permet à votre fonction de fonctionner pendant de longues périodes (jusqu'à un an) tout en maintenant une progression fiable malgré les interruptions.

Comment fonctionne le replay

Lambda conserve un journal de toutes les opérations durables (étapes, attentes et autres opérations) pendant l'exécution de votre fonction. Lorsque votre fonction doit faire une pause ou rencontre une interruption, Lambda enregistre ce journal des points de contrôle et arrête l'exécution. Au moment de reprendre, Lambda invoque à nouveau votre fonction depuis le début et rejoue le journal des points de contrôle, en remplaçant les valeurs stockées par les opérations terminées. Cela signifie que votre code s'exécute à nouveau, mais que les étapes précédemment effectuées ne sont pas réexécutées. Leurs résultats enregistrés sont utilisés à la place.

Ce mécanisme de rediffusion est fondamental pour comprendre les fonctions durables. Votre code doit être déterministe pendant la rediffusion, c'est-à-dire qu'il produit les mêmes résultats avec les mêmes entrées. Évitez les opérations comportant des effets secondaires (comme la génération de nombres aléatoires ou l'obtention de l'heure actuelle) en dehors des étapes, car elles peuvent produire des valeurs différentes pendant la rediffusion et provoquer un comportement non déterministe.

DurableContext

DurableContext est l'objet de contexte que reçoit votre fonction durable. Il fournit des méthodes pour des opérations durables, telles que des étapes et des attentes qui créent des points de contrôle et gèrent le flux d'exécution.

Votre fonction durable bénéficie d'un `DurableContext` au lieu du contexte Lambda par défaut :

TypeScript

```
import {
  DurableContext,
  withDurableExecution,
} from "@aws/durable-execution-sdk-js";

export const handler = withDurableExecution(
  async (event: any, context: DurableContext) => {
    const result = await context.step(async () => {
      return "step completed";
    });
    return result;
  },
);
```

Python

```
from aws_durable_execution_sdk_python import (
    DurableContext,
    durable_execution,
    durable_step,
)

@durable_step
def my_step(step_context, data):
```

```
    # Your business logic
    return result

@durable_execution
def handler(event, context: DurableContext):
    result = context.step(my_step(event["data"]))
    return result
```

À travers `DurableContext`, votre fonction a accès à des opérations durables qui permettent de contrôler la progression et de coordonner le travail :

- Étapes exécutez une logique métier avec de nouvelles tentatives intégrées et des points de contrôle automatiques. Chaque étape enregistre son résultat, de sorte que votre fonction reprend depuis la dernière étape terminée après une interruption.
- Attend sont des pauses planifiées au cours desquelles votre fonction s'arrête de fonctionner et arrête de se recharger jusqu'à ce qu'il soit temps de continuer. Utilisez-les pour des périodes, des rappels externes ou pour interroger une condition.
- Invoquer appelle d'autres fonctions Lambda, y compris des fonctions durables, et vérifie le résultat. Cross-account les invocations ne sont pas prises en charge.

Pour la référence linguistique complète de toutes les opérations durables disponibles, voir Référence du SDK dans le AWS Guide du développeur du SDK Durable Execution.

Configuration fonctionnelle durable

Les fonctions durables ajoutent des paramètres de configuration qui contrôlent le comportement d'exécution et la conservation des données. Ces paramètres s'ajoutent à la configuration existante de la fonction, telle que la mémoire et le délai d'expiration de la fonction. Elles s'appliquent à l'ensemble de l'exécution durable plutôt qu'à des invocations individuelles.

Le DurableConfig L'objet définit la configuration des fonctions durables :

```
{
  "ExecutionTimeout": Integer,
  "RetentionPeriodInDays": Integer
}
```

Execution timeout (Délai d’exécution)

Le délai d'exécution contrôle la durée pendant laquelle une exécution durable peut s'exécuter du début à la fin. Ceci est différent du délai d'expiration de la fonction Lambda, qui contrôle la durée pendant laquelle une seule invocation de fonction peut s'exécuter.

Une exécution durable peut couvrir plusieurs appels de fonctions Lambda au fur et à mesure de sa progression à travers les points de contrôle, les attentes et les rediffusions. Le délai d'exécution s'applique au temps total écoulé pendant l'exécution durable, et non aux appels de fonctions individuels.

Comprendre la différence

Le délai d'expiration de la fonction limite chaque appel individuel de votre fonction, jusqu'à 15 minutes par défaut ou 90 minutes pour les appels asynchrones et de mappage de sources d'événements sur les instances gérées Lambda. Le délai d'exécution durable (maximum 1 an) limite la durée totale entre le début de l'exécution et sa fin, son échec ou son expiration. Au cours de cette période, votre fonction peut être invoquée plusieurs fois pendant qu'elle traite les étapes, attend et se rétablit en cas d'échec.

Par exemple, si vous définissez un délai d'exécution durable de 24 heures et un délai d'expiration de la fonction Lambda de 5 minutes :

- Chaque appel de fonction doit être terminé dans les 5 minutes
- L'ensemble de l'exécution durable peut durer jusqu'à 24 heures
- Votre fonction peut être invoquée plusieurs fois au cours de ces 24 heures
- Les opérations d'attente ne sont pas prises en compte dans le délai d'expiration de la fonction Lambda mais dans le délai d'exécution

Vous pouvez configurer le délai d'exécution lors de la création d'une fonction durable à l'aide de la console Lambda, AWS CLI, ou AWS SAM. Dans la console Lambda, choisissez votre fonction, puis Configuration, Exécution durable. Définissez la valeur du délai d'exécution en secondes (par défaut : 86 400 secondes/24 heures, minimum : 60 secondes, maximum : 31536 000 secondes/1 an).

> **Note**
>
> Le délai d'exécution et le délai d'expiration de la fonction sont des paramètres différents. Le délai d'expiration de la fonction limite chaque appel, jusqu'à 15 minutes par défaut ou

90 minutes pour les appels asynchrones et de mappage de sources d'événements sur les instances gérées Lambda. Le délai d'exécution limite la durée totale de l'exécution durable sur toutes ses invocations (maximum 1 an).

Période de conservation

Le période de conservation contrôle la durée pendant laquelle Lambda conserve l'historique des exécutions et les données des points de contrôle après la fin d'une exécution durable. Ces données incluent les résultats des étapes, l'état d'exécution et le journal complet des points de contrôle.

À l'expiration de la période de conservation, Lambda supprime l'historique des exécutions et les données des points de contrôle. Vous ne pouvez plus récupérer les détails de l'exécution ni rejouer l'exécution. La période de rétention commence lorsque l'exécution atteint un état terminal (SUCCEDED, FAILED, STOPPED ou TIMED_OUT).

Vous pouvez configurer la période de rétention lors de la création d'une fonction durable à l'aide de la console Lambda, AWS CLI, ou AWS SAM. Dans la console Lambda, choisissez votre fonction, puis Configuration, Exécution durable. Définissez la valeur de la période de rétention en jours (par défaut : 14 jours, minimum : 1 jour, maximum : 90 jours).

Choisissez une période de rétention en fonction de vos exigences de conformité, de vos besoins en matière de débogage et de considérations financières. Des périodes de conservation plus longues permettent de consacrer plus de temps au débogage et à l'audit, mais augmentent les coûts de stockage.

Consultez aussi

- AWS Guide du développeur du SDK Durable Execution — Référence complète du SDK, didacticiels de démarrage rapide, cadre de test et guides spécifiques à une langue.
- Fonctions durables ou fonctions par étapes — Comparez les fonctions durables avec les fonctions par étapes pour comprendre quand chaque approche est la plus efficace.

Création de fonctions Lambda durables

Pour commencer à utiliser les fonctions durables Lambda, utilisez la console Lambda pour créer une fonction durable. En quelques minutes, vous pouvez créer et déployer une fonction durable qui utilise des étapes et des temps d'attente pour démontrer une exécution basée sur des points de contrôle.

Vous pouvez également créer des fonctions durables à l'aide de l'infrastructure AWS CLIor en tant que code (IaC).

Au cours de ce didacticiel, vous découvrirez les concepts fondamentaux des fonctions durables, tels que la façon d'utiliser l'`DurableContext`objet, de créer des points de contrôle avec des étapes et de suspendre l'exécution avec des temps d'attente. Vous découvrirez également comment fonctionne le replay lorsque votre fonction reprend après une attente.

Pour simplifier les choses, ce didacticiel vous montre comment créer votre fonction à l'aide de Python ou du Node.js runtime. Avec ces langages interprétés, vous pouvez modifier le code de fonction directement dans l'éditeur de code intégré à la console.

> **Note**
>
> Les fonctions durables prennent actuellement en charge les environnements d'exécution Python, Node.js (JavaScript/TypeScript) et Java, ainsi que les images de conteneur (OCI). Pour obtenir la liste complète des versions d'exécution et des options d'image de conteneur prises en charge, voir Runtimes pris en charge pour des fonctions durables. Pour plus d'informations sur l'utilisation d'images de conteneur avec Lambda, consultez la section Création d'images de conteneur Lambda dans le guide du développeur Lambda.

> **Tip**
>
> Pour apprendre à créer des solutions sans serveur, consultez le Guide du développeur sans serveur.

Créez une fonction Lambda durable avec la console

Dans cet exemple, votre fonction durable traite une commande en plusieurs étapes avec point de contrôle automatique. La fonction prend un objet JSON contenant un numéro de commande, valide la commande, traite le paiement et confirme la commande. Chaque étape est automatiquement contrôlée. Ainsi, si la fonction est interrompue, elle reprend à partir de la dernière étape terminée.

Votre fonction illustre également une opération d'attente, interrompant l'exécution pendant une courte période pour simuler l'attente d'une confirmation externe.

Pour créer une fonction durable avec la console

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez Create Event Function.
3. Sélectionnez Créer à partir de zéro.
4. Dans le volet Informations de base, pour Nom de la fonction, saisissez **`myDurableFunction`**.
5. Pour Runtime, choisissez Node.js 24 ou Python 3.14.
6. Sélectionnez Activer l'exécution durable.

Lambda crée votre fonction durable avec un rôle d'exécution qui inclut des autorisations pour les opérations de point de contrôle (`lambda:CheckpointDurableExecution`et). `lambda:GetDurableExecutionState`

> **Note**
>
> Les environnements d'exécution Lambda incluent le SDK Durable Execution, qui vous permet de tester des fonctions durables sans créer de dépendances. Toutefois, nous vous recommandons d'inclure le SDK dans votre package de déploiement pour la production. Cela garantit la cohérence des versions et évite les mises à jour d'exécution potentielles susceptibles d'affecter votre fonction.

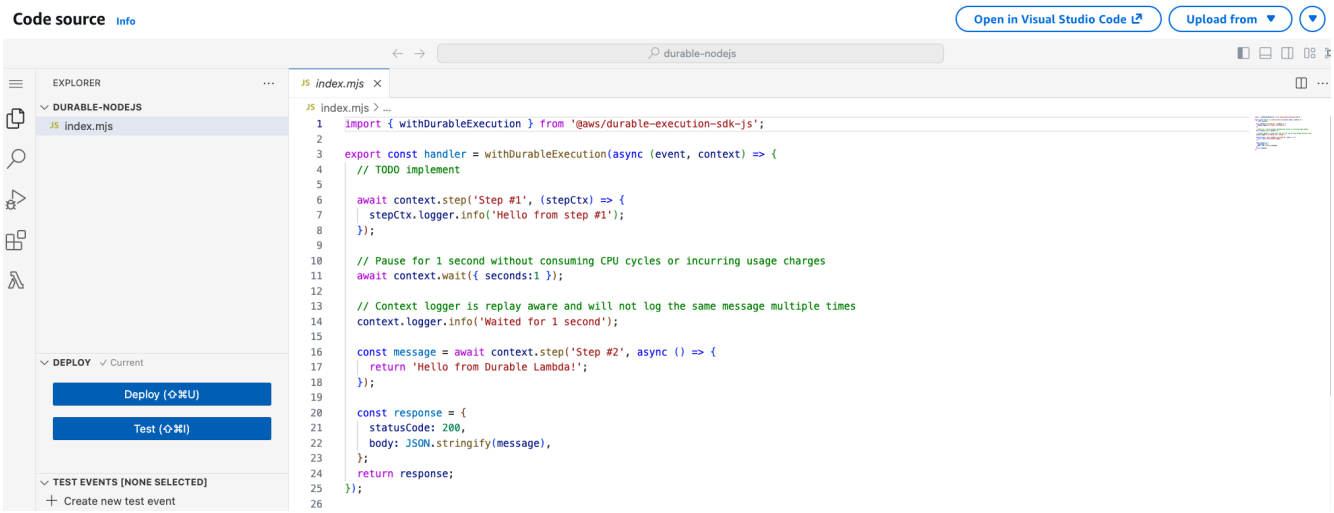
Utilisez l'éditeur de code intégré à la console pour ajouter votre code de fonction durable.

Node.js

Pour modifier le code dans la console

1. Cliquez sur l’onglet Code.

   Dans l'éditeur de code intégré de la console, vous devriez voir le code de fonction créé par Lambda. Si vous ne voyez pas l'onglet index.mjs dans l'éditeur de code, sélectionnez index.mjs dans l'explorateur de fichiers, comme le montre le schéma suivant.

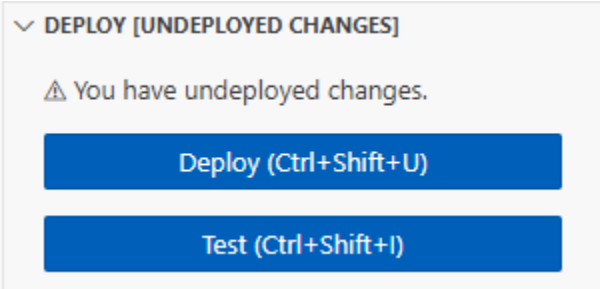


2. Collez le code suivant dans l'onglet index.mjs, en remplaçant le code créé par Lambda.

```
import {
  withDurableExecution,
} from "@aws/durable-execution-sdk-js";

export const handler = withDurableExecution(
  async (event, context) => {
    const orderId = event.orderId;

    // Step 1: Validate order
    const validationResult = await context.step(async (stepContext) => {
      stepContext.logger.info(`Validating order ${orderId}`);
      return { orderId, status: "validated" };
    });

    // Step 2: Process payment
    const paymentResult = await context.step(async (stepContext) => {
      stepContext.logger.info(`Processing payment for order ${orderId}`);
      return { orderId, status: "paid", amount: 99.99 };
    });

    // Wait for 10 seconds to simulate external confirmation
    await context.wait({ seconds: 10 });

    // Step 3: Confirm order
    const confirmationResult = await context.step(async (stepContext) => {
      stepContext.logger.info(`Confirming order ${orderId}`);
      return { orderId, status: "confirmed" };
    });
```

```
    return {
      orderId: orderId,
      status: "completed",
      steps: [validationResult, paymentResult, confirmationResult]
    };
  }
);
```

3. Dans la section DÉPLOYER, choisissez Déployer pour mettre à jour le code de votre fonction :



Comprendre votre code de fonction durable

Avant de passer à l'étape suivante, examinons le code de la fonction et comprenons les principaux concepts relatifs aux fonctions durables.

- L'`withDurableExecution`emballage :

  Votre fonction durable est emballée avec`withDurableExecution`. Ce wrapper permet une exécution durable en fournissant l'`DurableContext`objet et en gérant les opérations des points de contrôle.

- L'`DurableContext`objet :

  Au lieu du contexte Lambda standard, votre fonction reçoit un. `DurableContext` Cet objet fournit des méthodes pour des opérations durables telles `wait()` que `step()` et qui créent des points de contrôle.

- Étapes et points de contrôle :

  Chaque `context.step()` appel crée un point de contrôle avant et après l'exécution. Si votre fonction est interrompue, elle reprend à partir du dernier point de contrôle terminé. La fonction ne réexécute pas les étapes terminées. Il utilise plutôt leurs résultats enregistrés.

- Opérations d'attente :

  L'`context.wait()`appel interrompt l'exécution sans consommer de ressources informatiques. Une fois l'attente terminée, Lambda appelle à nouveau votre fonction et rejoue le journal des points de contrôle, en substituant des valeurs stockées aux étapes terminées.

- Mécanisme de rediffusion :

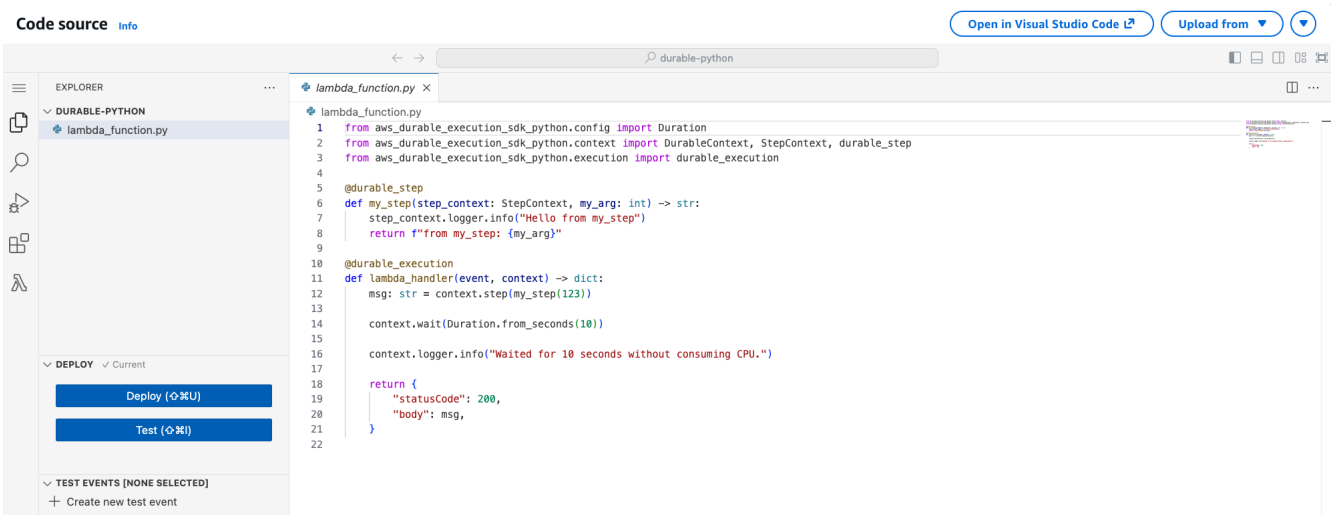
  Lorsque votre fonction reprend après une attente ou une interruption, Lambda exécute votre code depuis le début. Toutefois, les étapes terminées ne sont pas réexécutées. Lambda rejoue leurs résultats à partir du journal des points de contrôle. C'est pourquoi votre code doit être déterministe.

Python

Pour modifier le code dans la console

1. Cliquez sur l'onglet Code.

   Dans l'éditeur de code intégré de la console, vous devriez voir le code de fonction créé par Lambda. Si vous ne voyez pas l'onglet lambda_function.py dans l'éditeur de code, sélectionnez lambda_function.py dans l'explorateur de fichiers, comme le montre le schéma suivant.

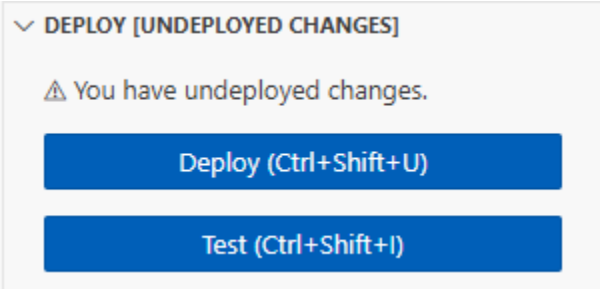


2. Collez le code suivant dans l'onglet lambda_function.py, en remplaçant le code créé par Lambda.

```
from aws_durable_execution_sdk_python import (
    DurableContext,
```

```
    durable_execution,
    durable_step,
)
from aws_durable_execution_sdk_python.config import Duration

@durable_step
def validate_order(step_context, order_id):
    step_context.logger.info(f"Validating order {order_id}")
    return {"orderId": order_id, "status": "validated"}

@durable_step
def process_payment(step_context, order_id):
    step_context.logger.info(f"Processing payment for order {order_id}")
    return {"orderId": order_id, "status": "paid", "amount": 99.99}

@durable_step
def confirm_order(step_context, order_id):
    step_context.logger.info(f"Confirming order {order_id}")
    return {"orderId": order_id, "status": "confirmed"}

@durable_execution
def lambda_handler(event, context: DurableContext):
    order_id = event['orderId']

    # Step 1: Validate order
    validation_result = context.step(validate_order(order_id))

    # Step 2: Process payment
    payment_result = context.step(process_payment(order_id))

    # Wait for 10 seconds to simulate external confirmation
    context.wait(Duration.from_seconds(10))

    # Step 3: Confirm order
    confirmation_result = context.step(confirm_order(order_id))

    return {
        "orderId": order_id,
        "status": "completed",
        "steps": [validation_result, payment_result, confirmation_result]
    }
```

3. Dans la section DÉPLOYER, choisissez Déployer pour mettre à jour le code de votre fonction :



Comprendre votre code de fonction durable

Avant de passer à l'étape suivante, examinons le code de la fonction et comprenons les principaux concepts relatifs aux fonctions durables.

- Le `@durable_execution` décorateur :

  Votre fonction de gestion est décorée avec`@durable_execution`. Ce décorateur permet une exécution durable en fournissant l'`DurableContext`objet et en gérant les opérations aux points de contrôle.
- Le `@durable_step` décorateur :

  Chaque fonction de marche est décorée avec`@durable_step`. Ce décorateur définit la fonction comme une étape durable qui crée des points de contrôle.
- L'`DurableContext`objet :

  Au lieu du contexte Lambda standard, votre fonction reçoit un. `DurableContext` Cet objet fournit des méthodes pour des opérations durables telles `wait()` que `step()` et qui créent des points de contrôle.
- Étapes et points de contrôle :

  Chaque `context.step()` appel crée un point de contrôle avant et après l'exécution. Si votre fonction est interrompue, elle reprend à partir du dernier point de contrôle terminé. La fonction ne réexécute pas les étapes terminées. Il utilise plutôt leurs résultats enregistrés.
- Opérations d'attente :

  L'`context.wait()`appel interrompt l'exécution sans consommer de ressources informatiques. Une fois l'attente terminée, Lambda appelle à nouveau votre fonction et rejoue le journal des points de contrôle, en substituant des valeurs stockées aux étapes terminées.
- Le SDK Python est synchrone :

Notez que le SDK Python n'utilise `await` pas. Toutes les opérations durables sont des appels de méthode synchrones.

Invoquez la fonction durable à l'aide de l'éditeur de code de la console

Lorsqu'aucune version explicite n'est spécifiée (ou publiée), la console invoque la fonction durable à l'aide du qualificatif de `$LATEST` version. Toutefois, pour une exécution déterministe de votre code, vous devez toujours utiliser un ARN qualifié pointant vers une version stable.

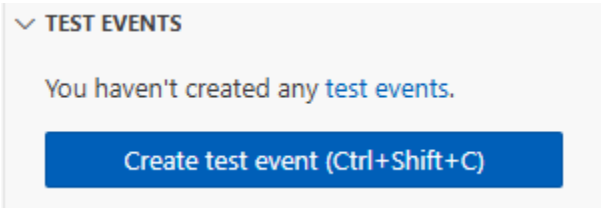
Pour publier une version de votre fonction

1. Choisissez l'onglet Versions.
2. Choisissez Publish new version (Publier une nouvelle version).
3. Dans le champ Description de la version, entrez **`Initial version`** (facultatif).
4. Choisissez Publier.
5. Lambda crée la version 1 de votre fonction. Notez que la fonction ARN inclut désormais `:1` à la fin, ce qui indique qu'il s'agit de la version 1.

Créez maintenant un événement de test à envoyer à votre fonction. L'événement est un document au format JSON contenant un numéro de commande.

Pour créer l'événement de test

1. Dans la section ÉVÉNEMENTS DE TEST de l'éditeur de code de console, choisissez Créer un événement de test.



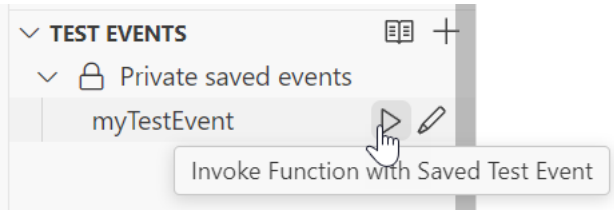
2. Dans Event Name (Nom de l'événement), saisissez **`myTestEvent`**.
3. Dans la section JSON d'événement, remplacez le JSON par défaut par ce qui suit :

```
{
  "orderId": "order-12345"
}
```

4. Cliquez sur Enregistrer.

Pour tester votre fonctionnalité durable et en voir l'exécution

Dans la section ÉVÉNEMENTS DE TEST de l'éditeur de code de la console, cliquez sur l'icône d'exécution à côté de votre événement de test :



Votre fonction durable commence à s'exécuter. Comme il inclut une attente de 10 secondes, l'appel initial se termine rapidement et la fonction reprend après la période d'attente. Vous pouvez consulter la progression de l'exécution dans l'onglet Exécutions durables.

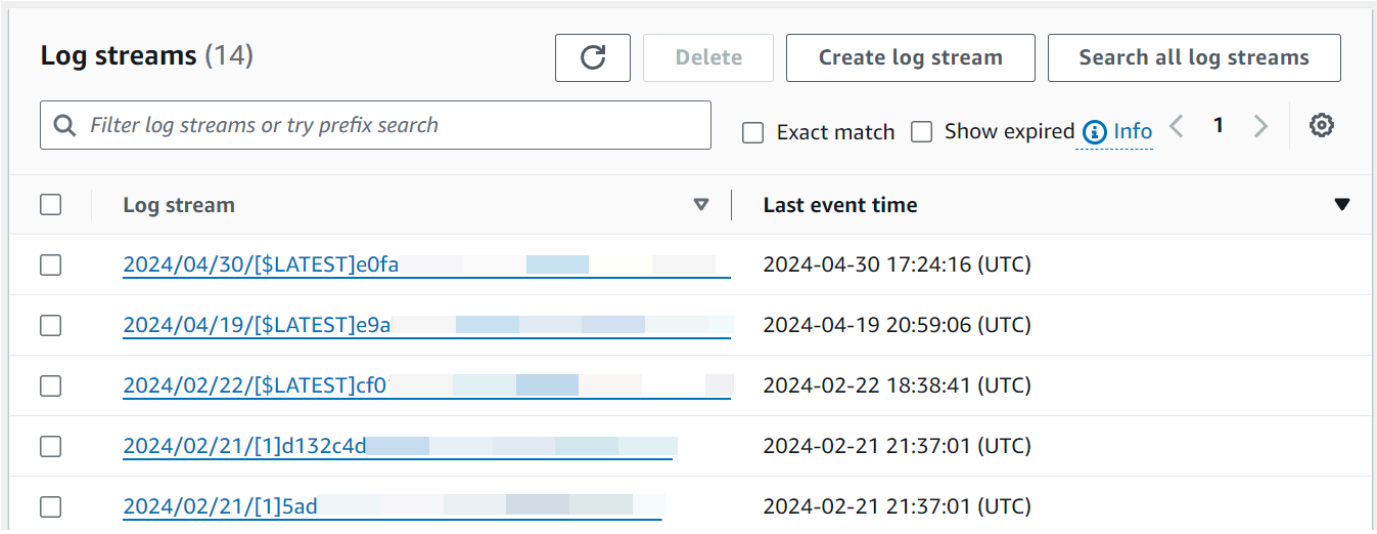
Pour visualiser l'exécution durable de vos fonctions

1. Choisissez l'onglet Exécutions durables.
2. Trouvez votre exécution dans la liste. L'exécution indique l'état actuel (en cours, réussi ou échec).
3. Choisissez l'ID d'exécution pour afficher les détails, notamment :
   - Chronologie d'exécution indiquant la date à laquelle chaque étape est terminée
   - Historique des points de contrôle
   - Périodes d'attente
   - Résultats des étapes

Vous pouvez également consulter les journaux de votre fonction dans CloudWatch Logs pour voir le résultat de chaque étape de la console.

Pour consulter les enregistrements d'invocation de votre fonction dans Logs CloudWatch

1. Ouvrez la page Groupes de journaux de la CloudWatch console.
2. Choisissez le groupe de journaux de votre fonction (`/aws/lambda/myDurableFunction`).
3. Faites défiler la page vers le bas et choisissez le flux de journaux pour les invocations de fonctions que vous souhaitez consulter.



Vous devriez voir des entrées de journal pour chaque appel de votre fonction, y compris l'exécution initiale et la rediffusion après l'attente.

> **Note**
>
> Lorsque vous utilisez l'enregistreur depuis `DurableContext` (tel que `context.logger` ou `stepContext.logger`), les journaux apparaissent également dans les vues d'exécution durable et d'étape de la console Lambda. Le chargement de ces journaux peut prendre un certain temps.

Nettoyage

Lorsque vous avez fini d'utiliser l'exemple de fonction durable, supprimez-le. Vous pouvez également supprimer le groupe de journaux qui stocke les journaux de la fonction, et le rôle d'exécution créé par la console.

Pour supprimer la fonction d'événement Lambda

1. Ouvrez la page Event Functions de la console Lambda.
2. Sélectionnez la fonction d'événement que vous avez créée.
3. Sélectionnez Actions, Supprimer.
4. Saisissez **`confirm`** dans la zone de saisie de texte et choisissez Delete (Supprimer).

Pour supprimer le groupe de journaux

1. Ouvrez la page Log groups (Groupes de journaux) de la console CloudWatch.
2. Sélectionnez le groupe de journaux de la fonction (`/aws/lambda/myDurableFunction`).
3. Sélectionnez Actions, Delete log group(s) (Supprimer le ou les groupes de journaux).
4. Dans la boîte de dialogue Delete log group(s) (Supprimer le ou les groupes de journaux), sélectionnez Delete (Supprimer).

Pour supprimer le rôle d'exécution

1. Ouvrez la page Rôles de la console Gestion des identités et des accès AWS (IAM).
2. Sélectionnez le rôle d'exécution de la fonction (par exemple, `myDurableFunction-role-31exxmpl`).
3. Sélectionnez Supprimer.
4. Dans la fenêtre de dialogue Supprimer le rôle, saisissez le nom du rôle, puis sélectionnez Supprimer.

Ressources supplémentaires et prochaines étapes

Maintenant que vous avez créé et testé une fonction simple et durable à l'aide de la console, procédez comme suit :

- Découvrez les cas d'utilisation courants des fonctions durables, notamment les transactions distribuées, le traitement des commandes et les flux de travail de révision humaine. Voir les exemples.
- Découvrez comment surveiller les exécutions de fonctions durables à l'aide de CloudWatch métriques et d'un historique d'exécution. Consultez la section Surveillance et débogage.
- Découvrez comment invoquer des fonctions durables de manière synchrone et asynchrone, et comment gérer les exécutions de longue durée. Voir Invocation de fonctions durables.
- Suivez les meilleures pratiques en matière de rédaction de code déterministe, de gestion de la taille des points de contrôle et d'optimisation des coûts. Consultez la section Bonnes pratiques.
- Découvrez comment tester des fonctions durables localement et dans le cloud. Voir Tester des fonctions durables.
- Comparez les fonctions durables aux Step Functions pour savoir quand chaque approche est la plus efficace. Voir Durable functions ou Step Functions.

Déployez et invoquez des fonctions durables Lambda avec AWS CLI

Utilisez le AWS CLI pour créer et déployer des fonctions Lambda durables avec des commandes impératives. Cette approche vous permet de contrôler directement chaque étape du processus de déploiement.

Conditions préalables

- Installez et configurez l' AWS CLI. Pour obtenir des instructions, reportez-vous à la section Installation du AWS CLI.
- Créez un package de déploiement avec votre code de fonction et le SDK d'exécution durable.
- Créez un rôle d'exécution IAM avec des autorisations de point de contrôle.

Créer le rôle d'exécution

Créez un rôle IAM avec des autorisations pour l'exécution Lambda de base et les opérations de point de contrôle.

Pour créer le rôle d'exécution

1. Créez un document de politique de confiance qui permet à Lambda d'assumer le rôle. Enregistrez ceci sous le nom `trust-policy.json` :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

2. Créez le rôle :

```
aws iam create-role \
  --role-name durable-function-role \
```

```
  --assume-role-policy-document file://trust-policy.json
```

3. Joignez la politique d'exécution durable pour les opérations de point de contrôle et l'exécution de base :

```
aws iam attach-role-policy \
  --role-name durable-function-role \
  --policy-arn arn:aws:iam::aws:policy/service-role/
AWSLambdaBasicDurableExecutionRolePolicy
```

La politique `AWSLambdaBasicDurableExecutionRolePolicy` gérée inclut les autorisations requises pour les opérations de point de contrôle (`lambda:CheckpointDurableExecution`et`lambda:GetDurableExecutionState`) et l'exécution de base de Lambda.

Créez une fonction durable

Créez votre fonction durable avec le `--durable-config` paramètre.

Pour créer une fonction durable

1. Package de votre code de fonction avec les dépendances dans un fichier .zip :

```
zip -r function.zip index.mjs node_modules/
```

> **Note**
>
> Pour les fonctions durables basées sur Java, vous devez compiler le code de votre fonction et ses dépendances dans un seul fichier .zip ou fichier Java Archive (JAR). Pour plus d'informations, voir Déployer des fonctions Java Lambda avec des archives de fichiers .zip ou JAR.

2. Créez la fonction avec l'exécution durable activée :

```
aws lambda create-function \
  --function-name myDurableFunction \
  --runtime nodejs22.x \
  --role arn:aws:iam::123456789012:role/durable-function-role \
  --handler index.handler \
  --zip-file fileb://function.zip \
```

```
  --durable-config '{"ExecutionTimeout": 3600, "RetentionPeriodInDays": 7}'
```

> **Note**
>
> Vous ne pouvez activer l'exécution durable que lors de la création de la fonction. Vous ne pouvez pas l'activer sur les fonctions existantes.

Publier une version

Bien que les fonctions durables puissent être invoquées à l'aide du qualificatif de `$LATEST` version, vous devez toujours utiliser un ARN qualifié pointant vers une version stable pour garantir une exécution déterministe de votre code.

```
aws lambda publish-version \
  --function-name myDurableFunction \
  --description "Initial version"
```

La commande renvoie l'ARN de la version. Notez le numéro de version (par exemple, `:1`) à la fin de l'ARN.

Vous pouvez éventuellement créer un alias pointant vers la version :

```
aws lambda create-alias \
  --function-name myDurableFunction \
  --name prod \
  --function-version 1
```

Invoquez la fonction durable

Appelez votre fonction durable à l'aide de l'ARN qualifié (version ou alias).

> **Note**
>
> Invocations idempotentes : pour éviter les doubles exécutions lors de nouvelles tentatives d'invocation infructueuses, vous pouvez fournir un nom d'exécution garantissant la sémantique d'exécution. at-most-once Voir Idempotency pour plus de détails.

Invocation synchrone

Pour les exécutions qui se terminent en 15 minutes, utilisez l'invocation synchrone :

```
aws lambda invoke \
  --function-name myDurableFunction:1 \
  --payload '{"orderId": "order-12345"}' \
  --cli-binary-format raw-in-base64-out \
  response.json
```

Ou en utilisant un alias :

```
aws lambda invoke \
  --function-name myDurableFunction:prod \
  --payload '{"orderId": "order-12345"}' \
  --cli-binary-format raw-in-base64-out \
  response.json
```

invocation asynchrone

Pour les exécutions de longue durée, utilisez l'invocation asynchrone :

```
aws lambda invoke \
  --function-name myDurableFunction:prod \
  --invocation-type Event \
  --payload '{"orderId": "order-12345"}' \
  --cli-binary-format raw-in-base64-out \
  response.json
```

En cas d'invocation asynchrone, Lambda revient immédiatement. La fonction continue de s'exécuter en arrière-plan.

> **Note**
>
> Vous pouvez l'utiliser `$LATEST` pour le prototypage et les tests dans la console. Pour les charges de travail de production, utilisez une version publiée ou un alias.

Gérez des exécutions durables

Utilisez les commandes suivantes pour gérer et surveiller les exécutions de fonctions durables.

Lister les exécutions

Répertoriez toutes les exécutions d'une fonction durable :

```
aws lambda list-durable-executions-by-function \
  --function-name myDurableFunction
```

Obtenir les détails de l'exécution

Obtenez des informations sur une exécution spécifique :

```
aws lambda get-durable-execution \
  --durable-execution-arn arn:aws:lambda:us-
east-1:123456789012:function:myDurableFunction:my-function-version/durable-execution/
my-execution-name/my-execution-id
```

Obtenir l'historique des exécutions

Consultez l'historique des points de contrôle d'une exécution :

```
aws lambda get-durable-execution-history \
  --durable-execution-arn arn:aws:lambda:us-
east-1:123456789012:function:myDurableFunction:my-function-version/durable-execution/
my-execution-name/my-execution-id
```

Arrêter une exécution

Arrêtez une exécution durable en cours :

```
aws lambda stop-durable-execution \
  --durable-execution-arn arn:aws:lambda:us-
east-1:123456789012:function:myDurableFunction:my-function-version/durable-execution/
my-execution-name/my-execution-id
```

Mettre à jour le code de la fonction

Mettez à jour votre code de fonction durable et publiez une nouvelle version :

Pour mettre à jour et publier une nouvelle version

1. Mettez à jour le code de fonction :

```
aws lambda update-function-code \
  --function-name myDurableFunction \
  --zip-file fileb://function.zip
```

2. Attendez que la mise à jour soit terminée :

```
aws lambda wait function-updated \
  --function-name myDurableFunction
```

3. Publiez une nouvelle version :

```
aws lambda publish-version \
  --function-name myDurableFunction \
  --description "Updated order processing logic"
```

4. Mettez à jour l'alias pour qu'il pointe vers la nouvelle version :

```
aws lambda update-alias \
  --function-name myDurableFunction \
  --name prod \
  --function-version 2
```

> **Important**
>
> Les exécutions en cours continuent à utiliser la version avec laquelle elles ont débuté. Les nouveaux appels utilisent la version mise à jour de l'alias.

Affichage des journaux de fonctions

Consultez les journaux de votre fonction durable dans CloudWatch Logs :

```
aws logs tail /aws/lambda/myDurableFunction --follow
```

Filtrez les journaux pour une exécution spécifique :

```
aws logs filter-log-events \
  --log-group-name /aws/lambda/myDurableFunction \
  --filter-pattern "exec-abc123"
```

nettoyer des ressources ;

Supprimez votre fonction durable et les ressources associées :

```
# Delete the function
aws lambda delete-function --function-name myDurableFunction

# Delete the IAM role policies
aws iam detach-role-policy \
  --role-name durable-function-role \
  --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole

aws iam detach-role-policy \
  --role-name durable-function-role \
  --policy-arn arn:aws:iam::aws:policy/service-role/
AWSLambdaBasicDurableExecutionRolePolicy

# Delete the role
aws iam delete-role --role-name durable-function-role
```

Étapes suivantes

Après avoir déployé votre fonction durable avec AWS CLI :

- Surveillez les exécutions à l'aide `list-durable-executions-by-function` des `get-durable-execution` commandes et
- Afficher les opérations des points de contrôle dans les événements de AWS CloudTrail données
- Configurer des CloudWatch alarmes en cas d'échec d'exécution ou d'exécutions de longue durée
- Automatisez les déploiements à l'aide de scripts shell ou CI/CD de pipelines

Pour plus d'informations sur AWS CLI les commandes pour Lambda, consultez la référence des AWS CLI commandes.

Déployez les fonctions durables de Lambda avec l'infrastructure en tant que code

Vous pouvez déployer des fonctions durables Lambda à l'aide d'outils d'infrastructure en tant que code (IaC) tels que AWS CloudFormation, AWS CDK AWS Serverless Application Model, ou Terraform. Ces outils vous permettent de définir votre fonction, votre rôle d'exécution et vos autorisations dans le code, ce qui permet de rendre les déploiements reproductibles et de contrôler les versions.

Les trois outils vous obligent à :

- Permettre une exécution durable de la fonction
- Accorder des autorisations de point de contrôle au rôle d'exécution
- Publiez une version ou créez un alias (les fonctions durables nécessitent des ARN qualifiés)

Fonctions durables grâce à une fermeture éclair

AWS CloudFormation

CloudFormation Utilisez-le pour définir votre fonction durable dans un modèle. L'exemple suivant crée une fonction durable avec les autorisations requises.

```
AWSTemplateFormatVersion: '2010-09-09'
Description: Lambda durable function example

Resources:
  DurableFunctionRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: '2012-10-17'
        Statement:
          - Effect: Allow
            Principal:
              Service: lambda.amazonaws.com
            Action: sts:AssumeRole
      ManagedPolicyArns:
        - arn:aws:iam::aws:policy/service-role/AWSLambdaBasicDurableExecutionRolePolicy

  DurableFunction:
    Type: AWS::Lambda::Function
    Properties:
      FunctionName: myDurableFunction
      Runtime: nodejs22.x
      Handler: index.handler
      Role: !GetAtt DurableFunctionRole.Arn
      Code:
        ZipFile: |
          // Your durable function code here
          export const handler = async (event, context) => {
            return { statusCode: 200 };
```

```
          };
      DurableConfig:
        ExecutionTimeout: 3600
        RetentionPeriodInDays: 7

  DurableFunctionVersion:
    Type: AWS::Lambda::Version
    Properties:
      FunctionName: !Ref DurableFunction
      Description: Initial version

  DurableFunctionAlias:
    Type: AWS::Lambda::Alias
    Properties:
      FunctionName: !Ref DurableFunction
      FunctionVersion: !GetAtt DurableFunctionVersion.Version
      Name: prod

Outputs:
  FunctionArn:
    Description: Durable function ARN
    Value: !GetAtt DurableFunction.Arn
  AliasArn:
    Description: Function alias ARN (use this for invocations)
    Value: !Ref DurableFunctionAlias
```

Pour déployer le modèle

```
aws cloudformation deploy \
  --template-file template.yaml \
  --stack-name my-durable-function-stack \
  --capabilities CAPABILITY_IAM
```

AWS CDK

Avec AWS CDK, vous pouvez définir l'infrastructure à l'aide de langages de programmation. Les exemples suivants montrent comment créer une fonction durable à l'aide TypeScript de Python.

TypeScript

```
import * as cdk from 'aws-cdk-lib';
import * as lambda from 'aws-cdk-lib/aws-lambda';
import * as iam from 'aws-cdk-lib/aws-iam';
```

```
import { Construct } from 'constructs';

export class DurableFunctionStack extends cdk.Stack {
  constructor(scope: Construct, id: string, props?: cdk.StackProps) {
    super(scope, id, props);

    // Create the durable function
    const durableFunction = new lambda.Function(this, 'DurableFunction', {
      runtime: lambda.Runtime.NODEJS_22_X,
      handler: 'index.handler',
      code: lambda.Code.fromAsset('lambda'),
      functionName: 'myDurableFunction',
      durableConfig: { executionTimeout: Duration.hours(1), retentionPeriod:
 Duration.days(30) },
    });

    // Create version and alias
    const version = durableFunction.currentVersion;
    const alias = new lambda.Alias(this, 'ProdAlias', {
      aliasName: 'prod',
      version: version,
    });

    // Output the alias ARN
    new cdk.CfnOutput(this, 'FunctionAliasArn', {
      value: alias.functionArn,
      description: 'Use this ARN to invoke the durable function',
    });
  }
}
```

Python

```
from aws_cdk import (
    Stack,
    aws_lambda as lambda_,
    aws_iam as iam,
    CfnOutput,
)
from constructs import Construct

class DurableFunctionStack(Stack):
    def __init__(self, scope: Construct, id: str, **kwargs):
```

```
        super().__init__(scope, id, **kwargs)

        # Create the durable function
        durable_function = lambda_.Function(
            self, 'DurableFunction',
            runtime=lambda_.Runtime.NODEJS_22_X,
            handler='index.handler',
            code=lambda_.Code.from_asset('lambda'),
            function_name='myDurableFunction',
            durable_execution={execution_timeout: Duration.hours(1),
 retention_period: Duration.days(30)}
        )

        # Add durable execution managed policy for checkpoint permissions
        durable_function.role.add_managed_policy(
            iam.ManagedPolicy.from_aws_managed_policy_name('service-role/
AWSLambdaBasicDurableExecutionRolePolicy')
        )

        # Create version and alias
        version = durable_function.current_version
        alias = lambda_.Alias(
            self, 'ProdAlias',
            alias_name='prod',
            version=version
        )

        # Output the alias ARN
        CfnOutput(
            self, 'FunctionAliasArn',
            value=alias.function_arn,
            description='Use this ARN to invoke the durable function'
        )
```

Pour déployer la pile CDK

```
cdk deploy
```

AWS Serverless Application Model

AWS SAM simplifie les CloudFormation modèles pour les applications sans serveur. Le modèle suivant crée une fonction durable avec AWS SAM.

```
AWSTemplateFormatVersion: '2010-09-09'
Transform: AWS::Serverless-2016-10-31
Description: Lambda durable function with SAM

Resources:
  DurableFunction:
    Type: AWS::Serverless::Function
    Properties:
      FunctionName: myDurableFunction
      Runtime: nodejs22.x
      Handler: index.handler
      CodeUri: ./src
      DurableConfig:
        ExecutionTimeout: 3600
        RetentionPeriodInDays: 7
      Policies:
        - arn:aws:iam::aws:policy/service-role/AWSLambdaBasicDurableExecutionRolePolicy
      AutoPublishAlias: prod

Outputs:
  FunctionArn:
    Description: Durable function ARN
    Value: !GetAtt DurableFunction.Arn
  AliasArn:
    Description: Function alias ARN (use this for invocations)
    Value: !Ref DurableFunction.Alias
```

Pour déployer le modèle SAM

```
sam build
sam deploy --guided
```

Terraform

Terraform est un outil IaC open source populaire qui prend en charge les ressources. AWS L'exemple suivant crée une fonction durable avec Terraform à l'aide de la version 6.25.0 ou ultérieure du AWS fournisseur.

```
terraform {
  required_version = ">= 1.0"
  required_providers {
    aws = {
```

```
      source  = "hashicorp/aws"
      version = ">= 6.25.0"
    }
  }
}

provider "aws" {
  region = "us-east-2"
}

# IAM Role for Lambda Function
resource "aws_iam_role" "lambda_role" {
  name = "durable-function-role"

  assume_role_policy = jsonencode({
    Version = "2012-10-17"
    Statement = [{
      Action = "sts:AssumeRole"
      Effect = "Allow"
      Principal = {
        Service = "lambda.amazonaws.com"
      }
    }]
  })
}

# Attach durable execution policy for checkpoint operations
resource "aws_iam_role_policy_attachment" "lambda_durable" {
  policy_arn = "arn:aws:iam::aws:policy/service-role/
AWSLambdaBasicDurableExecutionRolePolicy"
  role       = aws_iam_role.lambda_role.name
}

# Lambda Function with Durable Execution enabled
resource "aws_lambda_function" "durable_function" {
  filename      = "function.zip"
  function_name = "myDurableFunction"
  role          = aws_iam_role.lambda_role.arn
  handler       = "index.handler"
  runtime       = "nodejs22.x"
  timeout       = 30
  memory_size   = 512

  durable_config {
```

```
    execution_timeout = 900
    retention_period  = 7
  }
}

# Publish a version
resource "aws_lambda_alias" "prod" {
  name             = "prod"
  function_name    = aws_lambda_function.durable_function.function_name
  function_version = aws_lambda_function.durable_function.version
}

output "function_arn" {
  description = "ARN of the Lambda function"
  value       = aws_lambda_function.durable_function.arn
}

output "alias_arn" {
  description = "ARN of the function alias (use this for invocations)"
  value       = aws_lambda_alias.prod.arn
}
```

Pour déployer avec Terraform

```
terraform init
terraform plan
terraform apply
```

> **Note**
>
> La prise en charge par Terraform des fonctions durables de Lambda nécessite la version 6.25.0 AWS ou ultérieure du fournisseur. Mettez à jour la version de votre fournisseur si vous utilisez une ancienne version.

Fonctions durables à partir d'une image de conteneur OCI

Vous pouvez également créer des fonctions durables à partir d'images de conteneurs. Pour obtenir des instructions sur la création d'une image de conteneur, consultez la section Runtimes pris en charge pour des fonctions durables.

AWS CDK

Avec AWS CDK, vous pouvez définir l'infrastructure à l'aide de langages de programmation. Les exemples suivants montrent comment créer une fonction durable à TypeScript partir d'une image de conteneur.

```
import * as cdk from 'aws-cdk-lib';
import * as lambda from 'aws-cdk-lib/aws-lambda';
import * as iam from 'aws-cdk-lib/aws-iam';
import { Construct } from 'constructs';

export class DurableFunctionStack extends cdk.Stack {
  constructor(scope: Construct, id: string, props?: cdk.StackProps) {
    super(scope, id, props);

    // Create the durable function
    const durableFunction = new lambda.DockerImageFunction(this, 'DurableFunction', {
      code: lambda.DockerImageCode.fromImageAsset('./lambda', {
        platform: cdk.aws_ecr_assets.Platform.LINUX_AMD64,
      }),
      functionName: 'myDurableFunction',
      memorySize: 512,
      timeout: cdk.Duration.seconds(30),
      durableConfig: { executionTimeout: cdk.Duration.hours(1), retentionPeriod:
 cdk.Duration.days(30) },
    });

    // Create version and alias
    const version = durableFunction.currentVersion;
    const alias = new lambda.Alias(this, 'ProdAlias', {
      aliasName: 'prod',
      version: version,
    });

    // Output the alias ARN
    new cdk.CfnOutput(this, 'FunctionAliasArn', {
      value: alias.functionArn,
      description: 'Use this ARN to invoke the durable function',
    });
  }
}
```

Pour déployer la pile CDK

```
cdk deploy
```

AWS Serverless Application Model

AWS SAM simplifie les CloudFormation modèles pour les applications sans serveur. Le modèle suivant crée une fonction durable avec AWS SAM.

```
AWSTemplateFormatVersion: '2010-09-09'
Transform: AWS::Serverless-2016-10-31
Description: Lambda durable function with SAM

Resources:
  DurableFunction:
    Type: AWS::Serverless::Function
    Properties:
      FunctionName: myDurableFunction
      PackageType: Image
      ImageUri: ./src
      DurableConfig:
        ExecutionTimeout: 3600
        RetentionPeriodInDays: 7
      Policies:
        - arn:aws:iam::aws:policy/service-role/AWSLambdaBasicDurableExecutionRolePolicy
      AutoPublishAlias: prod
    Metadata:
      DockerTag: latest
      DockerContext: ./src
      Dockerfile: Dockerfile

Outputs:
  FunctionArn:
    Description: Durable function ARN
    Value: !GetAtt DurableFunction.Arn
  AliasArn:
    Description: Function alias ARN (use this for invocations)
    Value: !Ref DurableFunction.Alias
```

Pour déployer le modèle SAM

```
sam build
sam deploy --guided
```

Modèles de configuration courants

Quel que soit l'outil IaC que vous utilisez, suivez ces modèles pour des fonctions durables :

Permettre une exécution durable

Définissez la `DurableConfig` propriété de votre fonction pour permettre une exécution durable. Cette propriété n'est disponible que lors de la création de la fonction. Vous ne pouvez pas activer l'exécution durable sur les fonctions existantes.

Accorder des autorisations aux points de contrôle

Associez la politique `AWSLambdaBasicDurableExecutionRolePolicy` gérée au rôle d'exécution. Cette politique inclut les `lambda:GetDurableExecutionState` autorisations `lambda:CheckpointDurableExecution` et les autorisations requises.

Utilisez des ARN qualifiés

Créez une version ou un alias pour votre fonction. Les fonctions durables nécessitent des ARN qualifiés (avec version ou alias) pour être invoquées. Utilisez `AutoPublishAlias` AWS SAM ou créez des versions explicites dans CloudFormation AWS CDK, et Terraform.

Dépendances de package

Incluez le SDK d'exécution durable dans votre package de déploiement. Pour Node.js, installez`@aws/durable-execution-sdk-js`. Pour Python, installez`aws-durable-execution-sdk-python`.

Étapes suivantes

Après avoir déployé votre fonction durable :

- Testez votre fonction à l'aide de l'ARN qualifié (version ou alias)
- Surveillez la progression de l'exécution dans la console Lambda sous l'onglet Exécutions durables
- Afficher les opérations des points de contrôle dans les événements de AWS CloudTrail données
- Consultez CloudWatch les journaux pour connaître la sortie des fonctions et le comportement des rediffusions

Pour plus d'informations sur le déploiement de fonctions Lambda avec les outils IaC, consultez :

- CloudFormation AWS::Lambda: :Référence de fonction

- AWS CDK Documentation du module Lambda
- AWS SAM Manuel du développeur

Configurer les fonctions durables de Lambda

Les paramètres d'exécution durable contrôlent la durée pendant laquelle une exécution durable peut s'exécuter sur toutes ses invocations, la durée pendant laquelle l'historique des exécutions est AWS Lambda conservé et la AWS KMS clé qui chiffre vos données d'exécution. Configurez ces paramètres pour permettre une exécution durable de votre fonction.

Permettre une exécution durable

Configurez l'`DurableConfig`objet lors de la création de votre fonction pour définir le délai d'exécution et la conservation de l'historique. Vous ne pouvez activer l'exécution durable que lors de la création d'une fonction. Vous ne pouvez pas l'activer sur les fonctions existantes.

AWS CLI

```
aws lambda create-function \
  --function-name my-durable-function \
  --runtime nodejs24.x \
  --role arn:aws:iam::123456789012:role/my-durable-role \
  --handler index.handler \
  --zip-file fileb://function.zip \
  --durable-config '{"ExecutionTimeout": 3600, "RetentionPeriodInDays": 30,
 "KMSKeyArn": "arn:aws:kms:us-east-1:111122223333:key/key-id"}'
```

CloudFormation

```
Resources:
  MyDurableFunction:
    Type: AWS::Lambda::Function
    Properties:
      FunctionName: my-durable-function
      Runtime: nodejs24.x
      Handler: index.handler
      Code:
```

```
        ZipFile: |
          // Your durable function code
      DurableConfig:
        ExecutionTimeout: 3600
        RetentionPeriodInDays: 30
        KMSKeyArn: "arn:aws:kms:us-east-1:111122223333:key/key-id"
```

Paramètres de configuration :

- `ExecutionTimeout` : obligatoire. Durée maximale en secondes pendant laquelle une exécution durable peut être exécutée avant que Lambda n'arrête l'exécution. Ce délai s'applique à l'ensemble de l'exécution durable, et non aux invocations de fonctions individuelles. Vous devez le spécifier à `ExecutionTimeout` chaque fois que vous le fournissez `DurableConfig` ; la création d'une fonction avec une configuration durable mais aucun délai d'exécution échoue avec un`InvalidParameterValueException`. Plage valide : 1—31622400.
- `RetentionPeriodInDays` : facultatif. Nombre de jours pendant lesquels l'historique des exécutions est conservé après la fin d'une exécution durable. Après cette période, l'historique des exécutions n'est plus disponible via l'`GetDurableExecutionHistory`API. Plage valide : 1 à 90. Par défaut : 14.
- `KMSKeyArn` : facultatif. L'ARN d'une clé gérée par le client pour chiffrer les données d'exécution durables. Pour plus d'informations, consultez la section Chiffrement des données d'exécution durables de Lambda.

Pour la référence complète de l'API, voir la référence DurableConfigde l'API Lambda.

Bonnes pratiques en matière de configuration

Suivez les meilleures pratiques suivantes lors de la configuration de fonctions durables pour une utilisation en production :

- Définissez des délais d'exécution appropriés : configurez `ExecutionTimeout` en fonction de la durée maximale prévue de votre flux de travail. Ne fixez pas de délais d'attente inutilement longs, car ils affectent les coûts et l'allocation des ressources.
- Équilibrez la rétention avec les coûts de stockage : définissez les `RetentionPeriodInDays` paramètres en fonction de vos exigences en matière de débogage et d'audit. Des périodes de conservation plus longues augmentent les coûts de stockage.

- Taille de l'état du moniteur : les objets à état volumineux augmentent les coûts de stockage et peuvent avoir un impact sur les performances. Maintenez l'état minimal et utilisez un stockage externe pour les données volumineuses.
- Configurer une journalisation appropriée : activez la journalisation détaillée pour résoudre les problèmes liés aux flux de travail de longue durée, mais tenez compte de l'impact sur le volume des journaux et les coûts.
- Chiffrez avec votre propre AWS KMS clé : utilisez une clé gérée par le client pour contrôler la rotation des clés, auditer l'accès et répondre aux exigences de conformité. `KMSKeyArn` Consultez Chiffrement AWS Lambda données d'exécution durables.

Exemple de configuration de production :

```
{
  "ExecutionTimeout": 86400,
  "RetentionPeriodInDays": 7,
  "KMSKeyArn": "arn:aws:kms:us-east-1:111122223333:key/key-id"
}
```

Cet exemple définit un délai d'exécution de 24 heures (86 400 secondes), une période de rétention de 7 jours et une clé de chiffrement gérée par le client.

Fonctions durables ou Step Functions

Lambda est à la fois durable et AWS Step Functions permet une orchestration fiable des flux de travail avec gestion automatique des états et reprise en cas de panne. Ils répondent aux préférences des développeurs et à des modèles architecturaux différents. Les fonctions durables sont optimisées pour le développement d'applications dans Lambda, tandis que Step Functions est conçu pour l'orchestration des flux de travail entre les services. AWS

Quand utiliser des fonctions durables

Utilisez des fonctions durables lorsque :

- Votre équipe préfère les langages de programmation standard et les outils de développement familiers
- La logique de votre application réside principalement dans les fonctions Lambda

- Vous voulez un contrôle précis de l'état d'exécution du code
- Vous créez des applications centrées sur Lambda avec un lien étroit entre le flux de travail et la logique métier
- Vous souhaitez itérer rapidement sans passer du code aux concepteurs visual/JSON

Quand utiliser Step Functions

Utilisez Step Functions lorsque :

- Vous avez besoin d'une représentation visuelle du flux de travail pour une visibilité entre les équipes
- Vous orchestrez plusieurs AWS services et souhaitez des intégrations natives sans code SDK personnalisé
- Vous avez besoin d'une infrastructure ne nécessitant aucune maintenance (pas de correctifs, de mises à jour d'exécution)
- Les parties prenantes non techniques doivent comprendre et valider la logique du flux de travail

Cadre décisionnel

Posez-vous les questions suivantes pour déterminer quel service correspond à votre cas d'utilisation :

- Quel est votre objectif principal ? Développement d'applications dans Lambda → fonctions durables. Orchestration du flux de travail dans AWS → Step Functions.
- Quel est votre modèle de programmation préféré ? Langages de programmation standard → fonctions durables. DSL ou concepteur visuel basé sur des graphiques → Step Functions.
- Combien de AWS services sont concernés ? Lambda → fonctions durables principalement. AWS Services multiples → Step Functions.
- Quels outils de développement utilisez-vous ? Expérience de développeur Lambda, IDE avec agent LLM, frameworks de tests unitaires spécifiques au langage de programmation,, AWS SAM AWS CDK, AWS Toolkit → fonctions durables. Générateur de flux de travail visuel, AWS CDK pour modéliser les flux de travail → Step Functions.
- Qui gère l'infrastructure ? Vous recherchez de la flexibilité au sein de Lambda → des fonctions durables. Vous voulez une gestion complète, sans maintenance → Step Functions.

Comparaison des fonctionnalités

Le tableau suivant compare les principales fonctionnalités entre Step Functions et les fonctions durables Lambda :

Fonctionnalité	AWS Step Functions	Fonctions durables Lambda
Objectif principal	Orchestration du flux de travail à travers AWS	Développement d'applications dans Lambda
Type de service	Service de flux de travail autonome et dédié	Fonctionne dans Lambda
Modèle de programmation	Basé sur des graphiques, Amazon States Language DSL ou AWS CDK	Langages de programmation standard (JavaScript/TypeScript, Python)
Outils de développement	Générateur visuel dans l'extension IDE AWS Console/Toolkit, AWS CDK	Lambda DX dans les agents IDE et LLM, les frameworks de tests unitaires, l'extension IDE du Toolkit AWS SAM AWS
Intégrations	Plus de 220 AWS services, 16 000 APIs	Extension du modèle de programmation piloté par les événements Lambda (sources d'événements)
Gestion	Entièrement géré, indépendant du temps d'exécution, aucune maintenance (pas de correctifs, de mises à jour d'exécution)	Géré dans l'environnement Lambda
Idéal pour	Automatisation des processus métier et informatique, traitement des données, flux de travail basés sur l'IA	Transactions distribuées, logique d'application dynamique, orchestration des fonctions, traitement des données, flux de travail basés sur l'IA

Architectures hybrides

De nombreuses applications bénéficient de l'utilisation de ces deux services. Un modèle courant consiste à utiliser des fonctions durables pour la logique au niveau de l'application dans Lambda, tandis que Step Functions coordonne les flux de travail de haut niveau entre plusieurs services AWS au-delà des fonctions Lambda.

Considérations concernant la migration

Commencer par un processus simple et évolutif : commencez par des fonctions durables pour les flux de travail centrés sur Lambda. Ajoutez Step Functions lorsque vous avez besoin d'une orchestration multiservice ou d'une conception visuelle du flux de travail.

Utilisateurs existants de Step Functions : conservez Step Functions pour les flux de travail interservices établis. Envisagez des fonctions durables pour la nouvelle logique d'application Lambda qui a besoin de fiabilité.

Ressources connexes

- Fonctions durables Lambda
- Orchestration des fonctions Lambda avec Step Functions
- Commencer à utiliser des fonctions durables

Exemples et cas d'utilisation

Les fonctions durables de Lambda vous permettent de créer des applications en plusieurs étapes tolérantes aux pannes en utilisant des opérations durables telles que les étapes et les attentes. Grâce au point de contrôle automatique et au modèle de réexécution des points de contrôle, dans lequel l'exécution redémarre depuis le début après un échec mais ignore les points de contrôle terminés, vos fonctions peuvent se rétablir après un échec et reprendre l'exécution sans perdre leur progression.

> **Note**
>
> Pour obtenir des informations de référence sur l'API du SDK, des didacticiels de démarrage rapide, des guides spécifiques au langage et des modèles de flux de travail supplémentaires, consultez le Guide du développeur du SDK d'exécution AWS durable.

Short-lived processus tolérants aux pannes

Utilisez des fonctions durables pour créer des opérations fiables qui se terminent généralement en quelques minutes. Bien que ces processus soient plus courts que les flux de travail de longue durée, ils bénéficient tout de même du point de contrôle automatique et de la tolérance aux pannes dans les systèmes distribués. Des fonctions durables contribuent à garantir le succès de vos processus en plusieurs étapes, même en cas d'échec d'appels de service individuels, sans nécessiter de gestion des erreurs complexe ni de code de gestion des états.

Les scénarios courants incluent les systèmes de réservation d'hôtels, les plateformes de réservation de restaurants, les demandes de voyages en covoiturage, les achats de billets pour des événements et les mises à niveau d'abonnements SaaS. Ces scénarios présentent des caractéristiques communes : plusieurs appels de service qui doivent être exécutés simultanément, la nécessité d'une nouvelle tentative automatique en cas d'échec transitoire et la nécessité de maintenir un état cohérent sur l'ensemble des systèmes distribués.

Transactions distribuées sur des microservices

Coordonnez les paiements, les stocks et les expéditions entre plusieurs services grâce à l'annulation automatique en cas de panne. Chaque opération de service est encapsulée en une étape, ce qui garantit que la transaction peut être rétablie à tout moment en cas de défaillance d'un service.

TypeScript

```
import { DurableContext, withDurableExecution } from "@aws/durable-execution-sdk-
js";

export const handler = withDurableExecution(
  async (event: any, context: DurableContext) => {
    const { orderId, amount, items } = event;

    // Reserve inventory across multiple warehouses
    const inventory = await context.step("reserve-inventory", async () => {
      return await inventoryService.reserve(items);
    });

    // Process payment
    const payment = await context.step("process-payment", async () => {
      return await paymentService.charge(amount);
    });
```

```
    // Create shipment
    const shipment = await context.step("create-shipment", async () => {
      return await shippingService.createShipment(orderId, inventory);
    });

    return { orderId, status: 'completed', shipment };
  }
);
```

Python

```
from aws_durable_execution_sdk_python import DurableContext, durable_execution

@durable_execution
def lambda_handler(event, context: DurableContext):
    order_id = event['orderId']
    amount = event['amount']
    items = event['items']

    # Reserve inventory across multiple warehouses
    inventory = context.step(
        lambda _: inventory_service.reserve(items),
        name='reserve-inventory'
    )

    # Process payment
    payment = context.step(
        lambda _: payment_service.charge(amount),
        name='process-payment'
    )

    # Create shipment
    shipment = context.step(
        lambda _: shipping_service.create_shipment(order_id, inventory),
        name='create-shipment'
    )

    return {'orderId': order_id, 'status': 'completed', 'shipment': shipment}
```

Si une étape échoue, la fonction réessaie automatiquement à partir du dernier point de contrôle réussi. La réservation d'inventaire est maintenue même si le traitement du paiement échoue temporairement. Lorsque la fonction essaie à nouveau, elle ignore l'étape d'inventaire terminée et passe directement au traitement des paiements. Cela élimine les réservations dupliquées et garantit un état cohérent dans l'ensemble de votre système distribué.

Traitement des commandes en plusieurs étapes

Traitez les commandes par le biais de la validation, de l'autorisation de paiement, de l'allocation des stocks et de l'exécution avec une nouvelle tentative et une reprise automatiques. Chaque étape fait l'objet d'un point de contrôle, garantissant ainsi la progression de la commande même si les étapes individuelles échouent et que vous réessayez.

TypeScript

```
import { DurableContext, withDurableExecution } from "@aws/durable-execution-sdk-
js";

export const handler = withDurableExecution(
  async (event: any, context: DurableContext) => {
    const { orderId, customerId, items } = event;

    // Validate order details
    const validation = await context.step("validate-order", async () => {
      const customer = await customerService.validate(customerId);
      const itemsValid = await inventoryService.validateItems(items);
      return { customer, itemsValid };
    });

    if (!validation.itemsValid) {
      return { orderId, status: 'rejected', reason: 'invalid_items' };
    }

    // Authorize payment
    const authorization = await context.step("authorize-payment", async () => {
      return await paymentService.authorize(
        validation.customer.paymentMethod,
        calculateTotal(items)
      );
    });
```

```
    // Allocate inventory
    const allocation = await context.step("allocate-inventory", async () => {
      return await inventoryService.allocate(items);
    });

    // Fulfill order
    const fulfillment = await context.step("fulfill-order", async () => {
      return await fulfillmentService.createShipment({
        orderId,
        items: allocation.allocatedItems,
        address: validation.customer.shippingAddress
      });
    });

    return {
      orderId,
      status: 'completed',
      trackingNumber: fulfillment.trackingNumber
    };
  }
);
```

Python

```
from aws_durable_execution_sdk_python import DurableContext, durable_execution

@durable_execution
def lambda_handler(event, context: DurableContext):
    order_id = event['orderId']
    customer_id = event['customerId']
    items = event['items']

    # Validate order details
    def validate_order(_):
        customer = customer_service.validate(customer_id)
        items_valid = inventory_service.validate_items(items)
        return {'customer': customer, 'itemsValid': items_valid}

    validation = context.step(validate_order, name='validate-order')

    if not validation['itemsValid']:
```

```
        return {'orderId': order_id, 'status': 'rejected', 'reason':
'invalid_items'}

    # Authorize payment
    authorization = context.step(
        lambda _: payment_service.authorize(
            validation['customer']['paymentMethod'],
            calculate_total(items)
        ),
        name='authorize-payment'
    )

    # Allocate inventory
    allocation = context.step(
        lambda _: inventory_service.allocate(items),
        name='allocate-inventory'
    )

    # Fulfill order
    fulfillment = context.step(
        lambda _: fulfillment_service.create_shipment({
            'orderId': order_id,
            'items': allocation['allocatedItems'],
            'address': validation['customer']['shippingAddress']
        }),
        name='fulfill-order'
    )

    return {
        'orderId': order_id,
        'status': 'completed',
        'trackingNumber': fulfillment['trackingNumber']
    }
```

Ce modèle garantit que les commandes ne restent jamais bloquées dans des états intermédiaires. Si la validation échoue, la commande est rejetée avant l'autorisation de paiement. Si l'autorisation de paiement échoue, le stock n'est pas alloué. Chaque étape s'appuie sur la précédente avec une nouvelle tentative et une restauration automatiques.

Remarque

La vérification conditionnelle `if (!validation.itemsValid)` se situe en dehors d'une étape et est réexécutée pendant la rediffusion. C'est sûr car c'est déterministe : cela produit toujours le même résultat pour le même objet de validation.

Long-running processus

Utilisez des fonctions durables pour les processus qui s'étendent sur des heures, des jours ou des semaines. Les opérations d'attente suspendent l'exécution sans frais de calcul, ce qui permet de rentabiliser les processus de longue durée. Pendant les périodes d'attente, votre fonction cesse de fonctionner et Lambda recycle l'environnement d'exécution. Au moment de reprendre, Lambda invoque à nouveau votre fonction et la rejoue depuis le dernier point de contrôle.

Ce modèle d'exécution rend les fonctions durables idéales pour les processus qui doivent être interrompus pendant de longues périodes, qu'il s'agisse d'attendre des décisions humaines, des réponses du système externe, des fenêtres de traitement planifiées ou des retards temporels. Vous ne payez que pour le temps de calcul actif, et non pour le temps d'attente.

Les scénarios courants incluent les processus d'approbation des documents, le traitement par lots planifié, les processus d'intégration sur plusieurs jours, les processus d'essai d'abonnement et les systèmes de notification différée. Ces scénarios présentent des caractéristiques communes : des délais d'attente prolongés mesurés en heures ou en jours, la nécessité de maintenir l'état d'exécution pendant ces temps d'attente et des exigences liées aux coûts dans lesquelles le paiement pour le temps de calcul inactif est prohibitif.

Human-in-the-loop approbations

Suspendez l'exécution pour les révisions de documents, les approbations ou les décisions tout en maintenant l'état d'exécution. La fonction attend les rappels externes sans consommer de ressources et reprend automatiquement lorsque l'approbation est reçue.

Ce modèle est essentiel pour les processus qui nécessitent un jugement humain ou une validation externe. La fonction est suspendue au point de rappel, sans frais de calcul pendant l'attente. Lorsque quelqu'un soumet sa décision via l'API, Lambda invoque à nouveau votre fonction et rejoue depuis le point de contrôle, en continuant avec le résultat de l'approbation.

TypeScript

```
import { DurableContext, withDurableExecution } from "@aws/durable-execution-sdk-
js";
```

```
export const handler = withDurableExecution(
  async (event: any, context: DurableContext) => {
    const { documentId, reviewers } = event;

    // Step 1: Prepare document for review
    const prepared = await context.step("prepare-document", async () => {
      return await documentService.prepare(documentId);
    });

    // Step 2: Request approval with callback
    const approval = await context.waitForCallback(
      "approval-callback",
      async (callbackId) => {
        await notificationService.sendApprovalRequest({
          documentId,
          reviewers,
          callbackId,
          expiresIn: 86400
        });
      },
      {
        timeout: { seconds: 86400 }
      }
    );

    // Function resumes here when approval is received
    if (approval?.approved) {
      const finalized = await context.step("finalize-document", async () => {
        return await documentService.finalize(documentId, approval.comments);
      });

      return {
        status: 'approved',
        documentId,
        finalizedAt: finalized.timestamp
      };
    }

    // Handle rejection
    await context.step("archive-rejected", async () => {
      await documentService.archive(documentId, approval?.reason);
    });

    return {
```

```
      status: 'rejected',
      documentId,
      reason: approval?.reason
    };
  }
);
```

Python

```
from aws_durable_execution_sdk_python import DurableContext, durable_execution,
 WaitConfig

@durable_execution
def lambda_handler(event, context: DurableContext):
    document_id = event['documentId']
    reviewers = event['reviewers']

    # Step 1: Prepare document for review
    prepared = context.step(
        lambda _: document_service.prepare(document_id),
        name='prepare-document'
    )

    # Step 2: Request approval with callback
    def send_approval_request(callback_id):
        notification_service.send_approval_request({
            'documentId': document_id,
            'reviewers': reviewers,
            'callbackId': callback_id,
            'expiresIn': 86400
        })

    approval = context.wait_for_callback(
        send_approval_request,
        name='approval-callback',
        config=WaitConfig(timeout=86400)
    )

    # Function resumes here when approval is received
    if approval and approval.get('approved'):
        finalized = context.step(
```

```
            lambda _: document_service.finalize(document_id,
approval.get('comments')),
            name='finalize-document'
        )

        return {
            'status': 'approved',
            'documentId': document_id,
            'finalizedAt': finalized['timestamp']
        }

    # Handle rejection
    context.step(
        lambda _: document_service.archive(document_id, approval.get('reason') if
approval else None),
        name='archive-rejected'
    )

    return {
        'status': 'rejected',
        'documentId': document_id,
        'reason': approval.get('reason') if approval else None
    }
```

Lorsque le rappel est reçu et que votre fonction reprend, elle est rediffusée depuis le début. L'étape de préparation du document renvoie instantanément le résultat du point de contrôle. L'ForCallback opération d'attente renvoie également instantanément le résultat d'approbation enregistré au lieu d'attendre à nouveau. L'exécution se poursuit ensuite jusqu'aux étapes de finalisation ou d'archivage.

Multi-stage pipelines de données

Traitez de grands ensembles de données par le biais de phases d'extraction, de transformation et de chargement avec des points de contrôle entre les étapes. Chaque étape peut prendre des heures, et les points de contrôle permettent au pipeline de reprendre à partir de n'importe quelle étape en cas d'interruption.

Ce modèle est idéal pour les flux de travail ETL, les migrations de données ou les tâches de traitement par lots où vous devez traiter les données par étapes, avec des points de récupération entre eux. Si une étape échoue, le pipeline reprend à partir de la dernière étape terminée plutôt que de recommencer depuis le début. Vous pouvez également utiliser les opérations d'attente pour faire

une pause entre les étapes, en respectant les limites de débit, en attendant que les systèmes en aval soient prêts ou en planifiant le traitement en dehors des heures de pointe.

TypeScript

```
import { DurableContext, withDurableExecution } from "@aws/durable-execution-sdk-
js";

export const handler = withDurableExecution(
  async (event: any, context: DurableContext) => {
    const { datasetId, batchSize } = event;

    // Stage 1: Extract data from source
    const extracted = await context.step("extract-data", async () => {
      const records = await sourceDatabase.extractRecords(datasetId);
      return { recordCount: records.length, records };
    });

    // Wait 5 minutes to respect source system rate limits
    await context.wait({ seconds: 300 });

    // Stage 2: Transform data in batches
    const transformed = await context.step("transform-data", async () => {
      const batches = chunkArray(extracted.records, batchSize);
      const results = [];

      for (const batch of batches) {
        const transformed = await transformService.processBatch(batch);
        results.push(transformed);
      }

      return { batchCount: batches.length, results };
    });

    // Wait until off-peak hours (e.g., 2 AM)
    const now = new Date();
    const targetHour = 2;
    const msUntilTarget = calculateMsUntilHour(now, targetHour);
    await context.wait({ seconds: Math.floor(msUntilTarget / 1000) });

    // Stage 3: Load data to destination
    const loaded = await context.step("load-data", async () => {
```

```
      let loadedCount = 0;

      for (const result of transformed.results) {
        await destinationDatabase.loadBatch(result);
        loadedCount += result.length;
      }

      return { loadedCount };
    });

    // Stage 4: Verify and finalize
    const verified = await context.step("verify-pipeline", async () => {
      const verification = await destinationDatabase.verifyRecords(datasetId);
      await pipelineService.markComplete(datasetId, verification);
      return verification;
    });

    return {
      datasetId,
      recordsProcessed: extracted.recordCount,
      batchesProcessed: transformed.batchCount,
      recordsLoaded: loaded.loadedCount,
      verified: verified.success
    };
  }
);
```

Python

```
from aws_durable_execution_sdk_python import DurableContext, durable_execution
from datetime import datetime

@durable_execution
def lambda_handler(event, context: DurableContext):
    dataset_id = event['datasetId']
    batch_size = event['batchSize']

    # Stage 1: Extract data from source
    def extract_data(_):
        records = source_database.extract_records(dataset_id)
        return {'recordCount': len(records), 'records': records}
```

```
    extracted = context.step(extract_data, name='extract-data')

    # Wait 5 minutes to respect source system rate limits
    context.wait(Duration.from_seconds(300))

    # Stage 2: Transform data in batches
    def transform_data(_):
        batches = chunk_array(extracted['records'], batch_size)
        results = []

        for batch in batches:
            transformed = transform_service.process_batch(batch)
            results.append(transformed)

        return {'batchCount': len(batches), 'results': results}

    transformed = context.step(transform_data, name='transform-data')

    # Wait until off-peak hours (e.g., 2 AM)
    now = datetime.now()
    target_hour = 2
    ms_until_target = calculate_ms_until_hour(now, target_hour)
    context.wait(ms_until_target // 1000)

    # Stage 3: Load data to destination
    def load_data(_):
        loaded_count = 0

        for result in transformed['results']:
            destination_database.load_batch(result)
            loaded_count += len(result)

        return {'loadedCount': loaded_count}

    loaded = context.step(load_data, name='load-data')

    # Stage 4: Verify and finalize
    def verify_pipeline(_):
        verification = destination_database.verify_records(dataset_id)
        pipeline_service.mark_complete(dataset_id, verification)
        return verification

    verified = context.step(verify_pipeline, name='verify-pipeline')
```

```
    return {
        'datasetId': dataset_id,
        'recordsProcessed': extracted['recordCount'],
        'batchesProcessed': transformed['batchCount'],
        'recordsLoaded': loaded['loadedCount'],
        'verified': verified['success']
    }
```

Chaque étape est encapsulée dans une étape, ce qui crée un point de contrôle qui permet au pipeline de reprendre à partir de n'importe quelle étape en cas d'interruption. L'attente de 5 minutes entre l'extraction et la transformation respecte les limites de débit du système source sans consommer de ressources informatiques, tandis que l'attente jusqu'à 2 heures du matin permet de planifier l'opération de chargement coûteuse pendant les heures creuses.

Remarque

L'`new Date()`appel et la `calculateMsUntilHour()` fonction sont des étapes extérieures et sont réexécutés pendant la rediffusion. Pour les opérations basées sur le temps qui doivent être cohérentes entre les rediffusions, calculez l'horodatage d'une étape ou utilisez-le uniquement pour les durées d'attente (qui sont des points de contrôle).

Modèles avancés

Utilisez des fonctions durables pour créer des applications complexes en plusieurs étapes qui combinent plusieurs opérations durables, l'exécution parallèle, le traitement de tableaux, la logique conditionnelle et les interrogations. Ces modèles vous permettent de créer des applications sophistiquées qui coordonnent de nombreuses tâches tout en maintenant la tolérance aux pannes et la restauration automatique.

Les modèles avancés vont au-delà de simples étapes séquentielles. Vous pouvez exécuter des opérations simultanément`parallel()`, traiter des tableaux avec ces primitives`map()`, attendre des conditions externes et combiner ces primitives pour créer des applications fiables. `waitForCondition()` Chaque opération durable crée ses propres points de contrôle, afin que votre application puisse se rétablir à tout moment en cas d'interruption.

Processus d'intégration des utilisateurs

Guidez les utilisateurs lors de l'enregistrement, de la vérification des e-mails, de la configuration du profil et de la configuration initiale avec gestion des nouvelles tentatives. Cet exemple combine des étapes séquentielles, des rappels et une logique conditionnelle pour créer un processus d'intégration complet.

TypeScript

```
import { DurableContext, withDurableExecution } from "@aws/durable-execution-sdk-
js";

export const handler = withDurableExecution(
  async (event: any, context: DurableContext) => {
    const { userId, email } = event;

    // Step 1: Create user account
    const user = await context.step("create-account", async () => {
      return await userService.createAccount(userId, email);
    });

    // Step 2: Send verification email
    await context.step("send-verification", async () => {
      return await emailService.sendVerification(email);
    });

    // Step 3: Wait for email verification (up to 48 hours)
    const verified = await context.waitForCallback(
      "email-verification",
      async (callbackId) => {
        await notificationService.sendVerificationLink({
          email,
          callbackId,
          expiresIn: 172800
        });
      },
      {
        timeout: { seconds: 172800 }
      }
    );

    if (!verified) {
```

```
      await context.step("send-reminder", async () => {
        await emailService.sendReminder(email);
      });

      return {
        status: "verification_timeout",
        userId,
        message: "Email verification not completed within 48 hours"
      };
    }

    // Step 4: Initialize user profile in parallel
    const setupResults = await context.parallel("profile-setup", [
      async (ctx: DurableContext) => {
        return await ctx.step("create-preferences", async () => {
          return await preferencesService.createDefaults(userId);
        });
      },

      async (ctx: DurableContext) => {
        return await ctx.step("setup-notifications", async () => {
          return await notificationService.setupDefaults(userId);
        });
      },

      async (ctx: DurableContext) => {
        return await ctx.step("create-welcome-content", async () => {
          return await contentService.createWelcome(userId);
        });
      }
    ]);

    // Step 5: Send welcome email
    await context.step("send-welcome", async () => {
      const [preferences, notifications, content] = setupResults.getResults();
      return await emailService.sendWelcome({
        email,
        preferences,
        notifications,
        content
      });
    });

    return {
```

```
      status: "onboarding_complete",
      userId,
      completedAt: new Date().toISOString()
    };
  }
);
```

Python

```
from aws_durable_execution_sdk_python import DurableContext, durable_execution,
 WaitConfig
from datetime import datetime

@durable_execution
def lambda_handler(event, context: DurableContext):
    user_id = event['userId']
    email = event['email']

    # Step 1: Create user account
    user = context.step(
        lambda _: user_service.create_account(user_id, email),
        name='create-account'
    )

    # Step 2: Send verification email
    context.step(
        lambda _: email_service.send_verification(email),
        name='send-verification'
    )

    # Step 3: Wait for email verification (up to 48 hours)
    def send_verification_link(callback_id):
        notification_service.send_verification_link({
            'email': email,
            'callbackId': callback_id,
            'expiresIn': 172800
        })

    verified = context.wait_for_callback(
        send_verification_link,
        name='email-verification',
```

```
        config=WaitConfig(timeout=172800)
    )

    if not verified:
        context.step(
            lambda _: email_service.send_reminder(email),
            name='send-reminder'
        )

        return {
            'status': 'verification_timeout',
            'userId': user_id,
            'message': 'Email verification not completed within 48 hours'
        }

    # Step 4: Initialize user profile in parallel
    def create_preferences(ctx: DurableContext):
        return ctx.step(
            lambda _: preferences_service.create_defaults(user_id),
            name='create-preferences'
        )

    def setup_notifications(ctx: DurableContext):
        return ctx.step(
            lambda _: notification_service.setup_defaults(user_id),
            name='setup-notifications'
        )

    def create_welcome_content(ctx: DurableContext):
        return ctx.step(
            lambda _: content_service.create_welcome(user_id),
            name='create-welcome-content'
        )

    setup_results = context.parallel(
        [create_preferences, setup_notifications, create_welcome_content],
        name='profile-setup'
    )

    # Step 5: Send welcome email
    def send_welcome(_):
        results = setup_results.get_results()
        preferences, notifications, content = results[0], results[1], results[2]
        return email_service.send_welcome({
```

```
            'email': email,
            'preferences': preferences,
            'notifications': notifications,
            'content': content
        })

    context.step(send_welcome, name='send-welcome')

    return {
        'status': 'onboarding_complete',
        'userId': user_id,
        'completedAt': datetime.now().isoformat()
    }
```

Le processus combine des étapes séquentielles avec des points de contrôle pour la création de comptes et l'envoi d'e-mails, puis s'interrompt pendant 48 heures en attendant la vérification des e-mails sans consommer de ressources. La logique conditionnelle gère différents chemins selon que la vérification est terminée ou expirée. Les tâches de configuration du profil s'exécutent simultanément à l'aide d'opérations parallèles afin de réduire le temps d'exécution total, et chaque étape réessaie automatiquement en cas d'échec transitoire afin de garantir la fiabilité de l'intégration.

Invocations enchaînées entre les fonctions

Appelez d'autres fonctions Lambda depuis une fonction durable en utilisant. `context.invoke()` La fonction appelante est suspendue en attendant que la fonction invoquée soit terminée, créant ainsi un point de contrôle qui préserve le résultat. Si la fonction appelante est interrompue une fois la fonction invoquée terminée, elle reprend avec le résultat enregistré sans avoir à réinvoquer la fonction.

Utilisez ce modèle lorsque vous avez des fonctions spécialisées qui gèrent des domaines spécifiques (validation des clients, traitement des paiements, gestion des stocks) et que vous devez les coordonner dans un flux de travail. Chaque fonction conserve sa propre logique et peut être invoquée par plusieurs fonctions d'orchestrateur, évitant ainsi la duplication de code.

TypeScript

```
import { DurableContext, withDurableExecution } from "@aws/durable-execution-sdk-
js";

// Main orchestrator function
```

```
export const handler = withDurableExecution(
  async (event: any, context: DurableContext) => {
    const { orderId, customerId } = event;

    // Step 1: Validate customer by invoking customer service function
    const customer = await context.invoke(
      "validate-customer",
      "arn:aws:lambda:us-east-1:123456789012:function:customer-service:1",
      { customerId }
    );

    if (!customer.isValid) {
      return { orderId, status: "rejected", reason: "invalid_customer" };
    }

    // Step 2: Check inventory by invoking inventory service function
    const inventory = await context.invoke(
      "check-inventory",
      "arn:aws:lambda:us-east-1:123456789012:function:inventory-service:1",
      { orderId, items: event.items }
    );

    if (!inventory.available) {
      return { orderId, status: "rejected", reason: "insufficient_inventory" };
    }

    // Step 3: Process payment by invoking payment service function
    const payment = await context.invoke(
      "process-payment",
      "arn:aws:lambda:us-east-1:123456789012:function:payment-service:1",
      {
        customerId,
        amount: inventory.totalAmount,
        paymentMethod: customer.paymentMethod
      }
    );

    // Step 4: Create shipment by invoking fulfillment service function
    const shipment = await context.invoke(
      "create-shipment",
      "arn:aws:lambda:us-east-1:123456789012:function:fulfillment-service:1",
      {
        orderId,
        items: inventory.allocatedItems,
```

```
        address: customer.shippingAddress
      }
    );

    return {
      orderId,
      status: "completed",
      trackingNumber: shipment.trackingNumber,
      estimatedDelivery: shipment.estimatedDelivery
    };
  }
);
```

Python

```
from aws_durable_execution_sdk_python import DurableContext, durable_execution

# Main orchestrator function
@durable_execution
def lambda_handler(event, context: DurableContext):
    order_id = event['orderId']
    customer_id = event['customerId']

    # Step 1: Validate customer by invoking customer service function
    customer = context.invoke(
        'arn:aws:lambda:us-east-1:123456789012:function:customer-service:1',
        {'customerId': customer_id},
        name='validate-customer'
    )

    if not customer['isValid']:
        return {'orderId': order_id, 'status': 'rejected', 'reason':
 'invalid_customer'}

    # Step 2: Check inventory by invoking inventory service function
    inventory = context.invoke(
        'arn:aws:lambda:us-east-1:123456789012:function:inventory-service:1',
        {'orderId': order_id, 'items': event['items']},
        name='check-inventory'
    )
```

```
    if not inventory['available']:
        return {'orderId': order_id, 'status': 'rejected', 'reason':
'insufficient_inventory'}

    # Step 3: Process payment by invoking payment service function
    payment = context.invoke(
        'arn:aws:lambda:us-east-1:123456789012:function:payment-service:1',
        {
            'customerId': customer_id,
            'amount': inventory['totalAmount'],
            'paymentMethod': customer['paymentMethod']
        },
        name='process-payment'
    )

    # Step 4: Create shipment by invoking fulfillment service function
    shipment = context.invoke(
        'arn:aws:lambda:us-east-1:123456789012:function:fulfillment-service:1',
        {
            'orderId': order_id,
            'items': inventory['allocatedItems'],
            'address': customer['shippingAddress']
        },
        name='create-shipment'
    )

    return {
        'orderId': order_id,
        'status': 'completed',
        'trackingNumber': shipment['trackingNumber'],
        'estimatedDelivery': shipment['estimatedDelivery']
    }
```

Chaque invocation crée un point de contrôle dans la fonction d'orchestrateur. Si l'orchestrateur est interrompu une fois la validation du client terminée, il reprend à partir de ce point de contrôle avec les données client stockées, en ignorant l'appel de validation. Cela permet d'éviter les appels dupliqués vers les services en aval et de garantir une exécution cohérente malgré les interruptions.

La fonction invoquée peut être n'importe quelle fonction Lambda, y compris une fonction durable dotée de son propre flux de travail en plusieurs étapes, de ses propres temps d'attente et de ses

propres points de contrôle. La fonction appelante attend la fin de l'exécution durable, puis reçoit le résultat final.

> **Note**
>
> Cross-account les invocations ne sont pas prises en charge. Toutes les fonctions invoquées doivent être dans le même AWS compte que la fonction appelante.

Traitement par lots avec points de contrôle

Traitez des millions d'enregistrements grâce à la restauration automatique depuis le dernier point de contrôle réussi après un échec. Cet exemple montre comment les fonctions durables combinent les `map()` opérations avec le découpage et la limitation de débit pour gérer le traitement de données à grande échelle.

TypeScript

```
import { DurableContext, withDurableExecution } from "@aws/durable-execution-sdk-
js";

interface Batch {
  batchIndex: number;
  recordIds: string[];
}

export const handler = withDurableExecution(
  async (event: any, context: DurableContext) => {
    const { datasetId, batchSize = 1000 } = event;

    // Step 1: Get all record IDs to process
    const recordIds = await context.step("fetch-record-ids", async () => {
      return await dataService.getRecordIds(datasetId);
    });

    // Step 2: Split into batches
    const batches: Batch[] = [];
    for (let i = 0; i < recordIds.length; i += batchSize) {
      batches.push({
        batchIndex: Math.floor(i / batchSize),
        recordIds: recordIds.slice(i, i + batchSize)
```

```
      });
    }

    // Step 3: Process batches with controlled concurrency
    const batchResults = await context.map(
      "process-batches",
      batches,
      async (ctx: DurableContext, batch: Batch, index: number) => {
        const processed = await ctx.step(`batch-${batch.batchIndex}`, async () => {
          const results = [];
          for (const recordId of batch.recordIds) {
            const result = await recordService.process(recordId);
            results.push(result);
          }
          return results;
        });

        const validated = await ctx.step(`validate-${batch.batchIndex}`, async () =>
{
          return await validationService.validateBatch(processed);
        });

        return {
          batchIndex: batch.batchIndex,
          recordCount: batch.recordIds.length,
          successCount: validated.successCount,
          failureCount: validated.failureCount
        };
      },
      {
        maxConcurrency: 5
      }
    );

    // Step 4: Aggregate results
    const summary = await context.step("aggregate-results", async () => {
      const results = batchResults.getResults();
      const totalSuccess = results.reduce((sum, r) => sum + r.successCount, 0);
      const totalFailure = results.reduce((sum, r) => sum + r.failureCount, 0);

      return {
        datasetId,
        totalRecords: recordIds.length,
        batchesProcessed: batches.length,
```

```
        successCount: totalSuccess,
        failureCount: totalFailure,
        completedAt: new Date().toISOString()
      };
    });

    return summary;
  }
);
```

Python

```
from aws_durable_execution_sdk_python import DurableContext, durable_execution,
 MapConfig
from datetime import datetime
from typing import List, Dict

@durable_execution
def lambda_handler(event, context: DurableContext):
    dataset_id = event['datasetId']
    batch_size = event.get('batchSize', 1000)

    # Step 1: Get all record IDs to process
    record_ids = context.step(
        lambda _: data_service.get_record_ids(dataset_id),
        name='fetch-record-ids'
    )

    # Step 2: Split into batches
    batches = []
    for i in range(0, len(record_ids), batch_size):
        batches.append({
            'batchIndex': i // batch_size,
            'recordIds': record_ids[i:i + batch_size]
        })

    # Step 3: Process batches with controlled concurrency
    def process_batch(ctx: DurableContext, batch: Dict, index: int):
        batch_index = batch['batchIndex']

        def process_records(_):
```

```
            results = []
            for record_id in batch['recordIds']:
                result = record_service.process(record_id)
                results.append(result)
            return results

        processed = ctx.step(process_records, name=f'batch-{batch_index}')

        validated = ctx.step(
            lambda _: validation_service.validate_batch(processed),
            name=f'validate-{batch_index}'
        )

        return {
            'batchIndex': batch_index,
            'recordCount': len(batch['recordIds']),
            'successCount': validated['successCount'],
            'failureCount': validated['failureCount']
        }

    batch_results = context.map(
        process_batch,
        batches,
        name='process-batches',
        config=MapConfig(max_concurrency=5)
    )

    # Step 4: Aggregate results
    def aggregate_results(_):
        results = batch_results.get_results()
        total_success = sum(r['successCount'] for r in results)
        total_failure = sum(r['failureCount'] for r in results)

        return {
            'datasetId': dataset_id,
            'totalRecords': len(record_ids),
            'batchesProcessed': len(batches),
            'successCount': total_success,
            'failureCount': total_failure,
            'completedAt': datetime.now().isoformat()
        }

    summary = context.step(aggregate_results, name='aggregate-results')
```

```
    return summary
```

Les enregistrements sont divisés en lots gérables pour éviter de surcharger la mémoire ou les services en aval, puis plusieurs lots sont traités simultanément avec `maxConcurrency` le contrôle du parallélisme. Chaque lot possède son propre point de contrôle, de sorte que les échecs ne font que réessayer le lot défaillant au lieu de retraiter tous les enregistrements. Ce modèle est idéal pour les tâches ETL, les migrations de données ou les opérations en masse dont le traitement peut prendre des heures.

Étapes suivantes

- Explorez les concepts de base pour comprendre DurableContext, les étapes et les attentes
- Passez en revue les meilleures pratiques pour écrire du code déterministe et optimiser les performances
- Découvrez comment tester des fonctions durables en local et dans le cloud
- Comparez les fonctions durables aux Step Functions pour savoir quand chaque approche est la plus efficace. Voir Durable functions ou Step Functions.

Sécurité et autorisations pour les fonctions durables de Lambda

AWS Lambda les fonctions durables nécessitent des autorisations IAM spécifiques pour exécuter et gérer des exécutions durables. Suivez le principe du moindre privilège en n'accordant que les autorisations dont chaque directeur a besoin.

Autorisations IAM pour des fonctions durables

Pour la plupart des actions d'API d'exécution durables, Lambda autorise la demande sur l'ARN d'exécution durable, et non sur l'ARN de la fonction. Une exécution durable est une sous-ressource de la version d'une fonction, et son ARN étend l'ARN de la fonction :

`arn:aws:lambda:`*`region`*`:`*`account-id`*`:function:`*`function-name`*`:`*`qualifier`*`/durable-execution/`*`execution-name`*`/`*`execution-id`*

Le qualificatif d'un ARN d'exécution durable est toujours `$LATEST` ou un numéro de version.

Si votre politique spécifie un ARN de fonction non qualifié dans l'élément Resource, Lambda refuse la demande car un ARN non qualifié ne correspond jamais à un ARN d'exécution durable. Pour autoriser l'accès, ajoutez un modèle de qualificatif à la fonction ARN :

- `arn:aws:lambda:us-east-1:123456789012:function:my-function:*`— Correspond aux exécutions durables de chaque version.
- `arn:aws:lambda:us-east-1:123456789012:function:my-function:1/durable-execution/*`— Correspond aux exécutions durables de la version 1 uniquement.

La plupart des politiques utilisent le `:*` formulaire car les numéros de version peuvent changer à chaque déploiement.

> ⚠ Les alias ne s'appliquent pas aux autorisations d'exécution durables
>
> Vous pouvez invoquer une fonction durable via un alias, mais l'ARN de l'exécution qui en résulte contient le numéro de version résolu.

Autorisations du rôle d’exécution

Le rôle d'exécution de votre fonction durable doit être autorisé à créer des points de contrôle et à récupérer l'état d'exécution. La politique suivante indique les autorisations minimales requises :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "lambda:CheckpointDurableExecution",
                "lambda:GetDurableExecutionState"
            ],
            "Resource": "arn:aws:lambda:region:account-id:function:function-name:*"
        }
    ]
}
```

Lorsque vous créez une fonction durable à l'aide de la console, Lambda ajoute automatiquement ces autorisations au rôle d'exécution. Si vous créez la fonction à l'aide du AWS CLI ou AWS CloudFormation, ajoutez ces autorisations à votre rôle d'exécution.

Pour que Lambda assume votre rôle d'exécution, la politique de confiance du rôle doit spécifier le principal du service Lambda (`lambda.amazonaws.com`) en tant que service sécurisé. L'exemple suivant montre une politique de confiance qui accorde à Lambda l'autorisation d'assumer le rôle.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Principe du moindre privilège

Étendez l'`Resource`élément à des ARN de fonction spécifiques au lieu d'utiliser des caractères génériques. Cela limite le rôle d'exécution aux opérations de point de contrôle uniquement pour les fonctions qui en ont besoin.

Example Autorisations étendues pour plusieurs fonctions

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "lambda:CheckpointDurableExecution",
                "lambda:GetDurableExecutionState"
            ],
            "Resource": [
                "arn:aws:lambda:us-east-1:123456789012:function:orderProcessor:*",
                "arn:aws:lambda:us-east-1:123456789012:function:paymentHandler:*"
            ]
        }
    ]
}
```

Vous pouvez également utiliser la politique AWS gérée `AWSLambdaBasicDurableExecutionRolePolicy` qui inclut les autorisations d'exécution durables requises ainsi que les autorisations d'exécution Lambda de base pour Amazon CloudWatch Logs.

Autorisations pour la gestion des exécutions durables

Lambda autorise les `lambda:StopDurableExecution` actions `lambda:GetDurableExecutionlambda:GetDurableExecutionHistory`, et contre l'ARN d'exécution durable.

Pour répertorier les exécutions durables d'une fonction, utilise`lambda:ListDurableExecutionsByFunction`. Lambda autorise cette action sur la fonction ARN de la requête. Les règles suivantes s'appliquent à la correspondance des ARN :

- Une politique qui accorde à la fonction non qualifiée ARN ne correspond qu'aux requêtes qui utilisent le nom de la fonction non qualifiée.
- Une politique qui accorde un ARN qualifié ne fait correspondre que les requêtes qui utilisent un nom de fonction qualifié.

Pour de plus amples informations, veuillez consulter the section called “Fonctions de référencement dans la section Ressources relative aux stratégies”.

Pour faire correspondre les demandes faites avec l'une ou l'autre forme du nom de fonction, incluez à la fois l'ARN de la fonction non qualifiée et l'ARN de la fonction qualifiée, comme le montre la politique suivante :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ManageDurableExecutions",
            "Effect": "Allow",
            "Action": [
                "lambda:GetDurableExecution",
                "lambda:GetDurableExecutionHistory",
                "lambda:StopDurableExecution"
            ],
            "Resource": "arn:aws:lambda:us-
east-1:123456789012:function:myDurableFunction:*"
```

```
        },
        {
            "Sid": "ListDurableExecutions",
            "Effect": "Allow",
            "Action": "lambda:ListDurableExecutionsByFunction",
            "Resource": [
                "arn:aws:lambda:us-east-1:123456789012:function:myDurableFunction",
                "arn:aws:lambda:us-east-1:123456789012:function:myDurableFunction:*"
            ]
        }
    ]
}
```

Autorisations pour l'envoi de rappels

Le système externe qui envoie un résultat de rappel utilise les `lambda:SendDurableExecutionCallbackHeartbeat` actions `lambda:SendDurableExecutionCallbackSuccesslambda:SendDurableExecutionCallbackFai` et.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SendCallbacks",
            "Effect": "Allow",
            "Action": [
                "lambda:SendDurableExecutionCallbackSuccess",
                "lambda:SendDurableExecutionCallbackFailure",
                "lambda:SendDurableExecutionCallbackHeartbeat"
            ],
            "Resource": "arn:aws:lambda:us-
east-1:123456789012:function:myDurableFunction:*"
        }
    ]
}
```

Lambda autorise les demandes de rappel par rapport à l'ARN de l'exécution durable qui a créé le rappel.

Chiffrement d'état

Les fonctions durables Lambda chiffrent les données d'exécution au repos. Chaque exécution de fonction conserve un état isolé auquel les autres exécutions ne peuvent pas accéder. Vous pouvez configurer une clé gérée par le client pour chiffrer des données d'exécution durables. Pour de plus amples informations, veuillez consulter Chiffrement AWS Lambda données d'exécution durables.

Les données relatives aux points de contrôle incluent :

- Résultats des étapes et erreurs
- Entrées d'appel chaînées

Pour obtenir la liste complète des données d'exécution durables chiffrées au repos, consultezQu'est-ce qui est crypté.

Toutes les données sont chiffrées en transit à l'aide du protocole TLS lorsque Lambda lit ou écrit des données de point de contrôle.

Chiffrement personnalisé avec sérialiseurs et désérialiseurs personnalisés

Pour répondre à des exigences de sécurité critiques, vous pouvez implémenter votre propre mécanisme de chiffrement et de déchiffrement à l'aide de sérialiseurs et de désérialiseurs personnalisés () à l'aide d'un SDK durable. SerDer Cette approche vous donne un contrôle total sur les clés de chiffrement et les algorithmes utilisés pour protéger les données des points de contrôle.

> **Important**
>
> Lorsque vous utilisez le chiffrement personnalisé, vous perdez la visibilité des résultats des opérations dans la console Lambda et les réponses de l'API. Les données des points de contrôle apparaissent cryptées dans l'historique des exécutions et ne peuvent pas être inspectées sans déchiffrement.

Le rôle d'exécution de votre fonction nécessite `kms:Encrypt` et `kms:Decrypt` les autorisations nécessaires pour la AWS KMS clé utilisée dans l' SerDer implémentation personnalisée.

CloudTrail journalisation

Lambda enregistre les opérations aux points de contrôle en tant qu'événements de données dans. AWS CloudTrail Vous pouvez l'utiliser CloudTrail pour auditer la création de points de contrôle, suivre les changements d'état d'exécution et surveiller l'accès à des données d'exécution durables.

Les opérations relatives aux points de contrôle apparaissent dans CloudTrail les journaux avec les noms d'événements suivants :

- `CheckpointDurableExecution`- Enregistré lorsqu'une étape est terminée et crée un point de contrôle
- `GetDurableExecutionState`- Enregistré lorsque Lambda récupère l'état d'exécution pendant le replay

Pour activer la journalisation des événements de données pour les fonctions durables, configurez un journal CloudTrail pour enregistrer les événements de données Lambda. Pour plus d'informations, consultez la section Journalisation des événements liés aux données dans le Guide de CloudTrail l'utilisateur.

Exemple : entrée de CloudTrail journal pour le fonctionnement des points de contrôle

```
{
    "eventVersion": "1.08",
    "eventTime": "2024-11-16T10:30:45Z",
    "eventName": "CheckpointDurableExecution",
    "eventSource": "lambda.amazonaws.com",
    "requestParameters": {
        "functionName": "myDurableFunction",
        "executionId": "exec-abc123",
        "stepId": "step-1"
    },
    "responseElements": null,
    "eventType": "AwsApiCall"
}
```

Cross-account considérations

Si vous invoquez des fonctions durables sur plusieurs AWS comptes, le compte appelant a besoin d'une `lambda:InvokeFunction` autorisation, mais les opérations de point de contrôle utilisent

toujours le rôle d'exécution dans le compte de la fonction. Le compte appelant ne peut pas accéder directement aux données des points de contrôle ou à l'état d'exécution.

Cette isolation garantit la sécurité des données des points de contrôle dans le compte de la fonction, même lorsqu'elles sont invoquées depuis des comptes externes.

Fonctionnalités de sécurité Lambda héritées

Les fonctions durables héritent de toutes les fonctionnalités de sécurité, de gouvernance et de conformité de Lambda. Il s'agit notamment de la connectivité VPC, du chiffrement des variables d'environnement, des files d'attente de lettres mortes, de la simultanéité réservée, des URL de fonction, de la signature de code et des certifications de conformité telles que SOC, PCI DSS et HIPAA.

Pour obtenir des informations détaillées sur les fonctionnalités de sécurité de Lambda, consultez la section Security in AWS Lambda dans le Lambda Developer Guide. Les seules considérations de sécurité supplémentaires pour les fonctions durables sont les autorisations IAM documentées dans ce guide.

Chiffrement AWS Lambda données d'exécution durables

Grâce à des fonctions AWS Lambda durables, vous pouvez créer des applications résilientes en plusieurs étapes qui s'exécutent jusqu'à un an, en utilisant des points de contrôle pour récupérer chaque exécution en cas d'échec en rejouant le travail terminé.

Lambda chiffre toujours les données d'exécution durables au repos. Vous pouvez également configurer votre propre clé gérée par le AWS KMS client sur la fonction de contrôle de rotation, de visibilité des audits ou de conformité. Avec une clé gérée par le client, seuls les principaux que vous autorisez peuvent lire les données d'exécution.

Comment fonctionne le chiffrement

Une exécution durable Lambda utilise la même clé KMS avec laquelle elle a commencé pendant toute sa durée de vie. La modification ou la suppression de la touche de la fonction n'affecte que les exécutions qui démarrent après la modification. Découvrez Lorsque la clé gérée par le client n'est pas disponible comment se comporte une exécution durable lorsque sa clé n'est pas disponible.

Les clés gérées par le client entraînent des AWS KMS frais standard. Pour plus d’informations sur la tarification, consultez Tarification AWS Key Management Service.

Qu'est-ce qui est crypté

Lorsque vous configurez une clé gérée par le client sur une fonction durable, Lambda utilise cette clé pour chiffrer les données d'exécution durables suivantes au repos :

- La charge utile d'entrée que vous transmettez à chaque `Invoke` demande.
- Les données des points de contrôle sont conservées par l'`CheckpointDurableExecution`API, notamment les résultats des étapes, les erreurs d'étape et les entrées d'appel chaînées.
- Résultats d'exécution et erreurs.
- Résultats des rappels et erreurs que vous soumettez par le biais de `SendDurableExecutionCallbackSuccess` et`SendDurableExecutionCallbackFailure`.

> **Function-level et les clés d'exécution durables sont indépendantes**
>
> Le niveau de fonction `KMSKeyArn` qui chiffre les variables d'environnement, les packages de déploiement .zip et les SnapStartinstantanés est distinct de `DurableConfig` celui qui chiffre les données d'`KMSKeyArn`exécution durables. Régler l'un ne définit pas l'autre. Vous pouvez utiliser la même clé KMS pour les deux, ou vous pouvez utiliser des clés KMS différentes.

Configurer le chiffrement des clés géré par le client

La configuration du chiffrement par clé géré par le client pour une fonction durable est un processus en trois étapes. Effectuez les étapes suivantes dans l'ordre.

Création d'une clé gérée par le client

Les fonctions durables prennent en charge le chiffrement symétrique des clés KMS dans la même AWS région que la fonction. Cross-Region les touches ne sont pas prises en charge. Pour créer une clé symétrique gérée par le client, suivez les étapes de création de clés KMS de chiffrement symétriques décrites dans le guide du AWS Key Management Service développeur.

Permissions

Vous accordez AWS KMS des autorisations par le biais de la politique clé de la clé KMS.

La configuration d'une clé gérée par le client nécessite AWS KMS des autorisations sur le principal qui crée ou met à jour la fonction. L'invocation d'une fonction durable ne nécessite aucune AWS KMS autorisation de la part de l'appelant ; Lambda effectue le chiffrement avec son principal de service.

Stratégie de clé

Les stratégies de clé contrôlent l'accès à votre clé gérée par le client. Chaque clé gérée par le client doit avoir exactement une politique clé. Dans une politique de clé, `Resource: "*"` fait uniquement référence à la clé KMS à laquelle la politique est attachée, et non à toutes les clés KMS de votre compte.

La politique clé d'une fonction durable accorde à chaque principal uniquement les AWS KMS actions dont il a besoin, définies par l'ARN du service et de la fonction. Les sections suivantes décrivent les instructions, les conditions et un exemple complet.

Déclarations de politique requises

La politique accorde les fonctionnalités suivantes :

- Activez les autorisations des utilisateurs IAM. Accorde au root du compte un accès inconditionnel à la gestion de la clé. Cette instruction n'impose aucune condition, car son étendue vous empêcherait de faire pivoter, de mettre à jour ou de supprimer la clé.
- Autorisez Lambda à utiliser cette clé pour des fonctions durables. Accorde le principal `kms:GenerateDataKey` du service Lambda et. `kms:Decrypt`
- Autorisez le rôle d'exécution de la fonction à déchiffrer les données d'exécution durables. Accorde le rôle d'exécution `kms:Decrypt` pour lire l'état et faire avancer l'exécution.
- Permettez à l'auteur de la fonction de décrire cette clé. Des subventions `kms:DescribeKey` pour que Lambda puisse valider que la clé est symétrique et activée pendant ou. `CreateFunction` `UpdateFunctionConfiguration`
- Autorisez l'auteur de la fonction à valider cette clé pour une fonction spécifique. `kms:Decrypt`Ainsi, Lambda peut valider les autorisations clés et l'accès avec le contexte de chiffrement de la fonction pendant `CreateFunction` ou. `kms:GenerateDataKey` `UpdateFunctionConfiguration` Cela confirme que la politique des touches accepte les appels pour cette fonction spécifique avant que celle-ci ne soit créée ou mise à jour.
- Permettez aux opérateurs d'exécution durables. Accorde des opérateurs `kms:Decrypt` pour les appels vers `GetDurableExecutionIncludeExecutionData=true`, `GetDurableExecutionHistory` avec`GetDurableExecutionState`,`StopDurableExecution`, et les API de rappel.

Il est recommandé d'utiliser des principes distincts pour le rôle d'exécution, l'auteur de la fonction et l'opérateur d'exécution durable afin que chaque identité ne dispose que des fonctionnalités dont elle a besoin.

Conditions politiques recommandées

La politique utilise les conditions suivantes pour limiter l'accès :

- kms : ViaService limite l'utilisation des clés aux demandes acheminées via Lambda. L'application de cette méthode aux instructions du rôle d'exécution, de l'auteur de la fonction et de l'opérateur les empêche d'utiliser directement la clé AWS KMS.
- aws : SourceArn et aws : SourceAccount protègent contre le problème de confusion entre les services adjoints. Lambda transmet ces valeurs lorsqu'il appelle AWS KMS en utilisant ses propres informations d'identification de service. Cette condition s'applique uniquement à la déclaration principale du service Lambda. Les instructions relatives au rôle d'exécution, à l'auteur de la fonction et à l'opérateur appellent AWS KMS avec les informations d'identification de la session d'accès direct de l'appelant, qui ne contiennent pas ces en-têtes.
- kms : EncryptionContext:aws:lambda:FunctionArn délimite la clé d'une fonction spécifique. Lambda ajoute cela au contexte de chiffrement de chaque AWS KMS appel pour des données d'exécution durables.

L'exemple suivant combine les instructions et les conditions ci-dessus.

Example Politique clé pour des fonctions durables

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal": { "AWS": "arn:aws:iam::111122223333:root" },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Allow Lambda to use this key for durable functions",
            "Effect": "Allow",
            "Principal": { "Service": "lambda.amazonaws.com" },
            "Action": [ "kms:GenerateDataKey", "kms:Decrypt" ],
```

```
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333",
                    "aws:SourceArn": "arn:aws:lambda:us-
east-1:111122223333:function:myDurableFunction",
                    "kms:EncryptionContext:aws:lambda:FunctionArn": "arn:aws:lambda:us-
east-1:111122223333:function:myDurableFunction"
                }
            }
        },
        {
            "Sid": "Allow the function execution role to decrypt durable execution
 data",
            "Effect": "Allow",
            "Principal": { "AWS": "arn:aws:iam::111122223333:role/
myDurableFunctionRole" },
            "Action": "kms:Decrypt",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "lambda.us-east-1.amazonaws.com",
                    "kms:EncryptionContext:aws:lambda:FunctionArn": "arn:aws:lambda:us-
east-1:111122223333:function:myDurableFunction"
                }
            }
        },
        {
            "Sid": "Allow the function author to describe this key",
            "Effect": "Allow",
            "Principal": { "AWS": "arn:aws:iam::111122223333:role/FunctionAuthor" },
            "Action": "kms:DescribeKey",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "lambda.us-east-1.amazonaws.com"
                }
            }
        },
        {
            "Sid": "Allow the function author to validate this key for a specific
 function",
            "Effect": "Allow",
            "Principal": { "AWS": "arn:aws:iam::111122223333:role/FunctionAuthor" },
```

```
            "Action": [ "kms:GenerateDataKey", "kms:Decrypt" ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "lambda.us-east-1.amazonaws.com",
                    "kms:EncryptionContext:aws:lambda:FunctionArn": "arn:aws:lambda:us-
east-1:111122223333:function:myDurableFunction"
                }
            }
        },
        {
            "Sid": "Allow durable execution operators",
            "Effect": "Allow",
            "Principal": { "AWS": "arn:aws:iam::111122223333:role/
DurableExecutionOperator" },
            "Action": "kms:Decrypt",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "lambda.us-east-1.amazonaws.com",
                    "kms:EncryptionContext:aws:lambda:FunctionArn": "arn:aws:lambda:us-
east-1:111122223333:function:myDurableFunction"
                }
            }
        }
    ]
}
```

Pour plus d'informations sur les politiques AWS KMS clés, consultez Comment modifier une politique clé dans le Guide du AWS Key Management Service développeur.

Configuration d'une clé gérée par le client sur une fonction durable

Vous configurez la clé gérée par le client pour des données d'exécution durables via le `KMSKeyArn` champ de l'`DurableConfig`objet. Réglez-le lorsque vous créez la fonction avec CreateFunction; mettez-le à jour sur une fonction durable existante avec UpdateFunctionConfiguration.

Lambda console

Pour configurer une clé gérée par le client sur une fonction durable existante

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez une fonction durable.

3. Choisissez Configuration, puis Exécution durable dans la barre de navigation de gauche.
4. Choisissez Modifier.
5. Sous Chiffrement, choisissez Utiliser une clé gérée par le client, puis choisissez une clé KMS dans la liste.
6. Cliquez sur Enregistrer.

AWS CLI

Pour configurer une clé gérée par le client lorsque vous créez une fonction

Dans l'exemple de fonction de création suivant, l'`--durable-config`option spécifie l'ARN de la clé géré par le client ainsi que le délai d'exécution durable et la période de rétention.

```
aws lambda create-function \
  --function-name myDurableFunction \
  --runtime nodejs24.x \
  --handler index.handler \
  --role arn:aws:iam::111122223333:role/myDurableFunctionRole \
  --zip-file fileb://function.zip \
  --durable-config '{"KMSKeyArn":"arn:aws:kms:us-east-1:111122223333:key/key-
id","ExecutionTimeout":3600,"RetentionPeriodInDays":30}'
```

Pour configurer une clé gérée par le client sur une fonction durable existante

Utilisez la commande update-function-configuration. Incluez tous les `DurableConfig` champs que vous souhaitez conserver, car cela `--durable-config` remplace l'objet dans son intégralité.

```
aws lambda update-function-configuration \
  --function-name myDurableFunction \
  --durable-config '{"KMSKeyArn":"arn:aws:kms:us-east-1:111122223333:key/key-
id","ExecutionTimeout":3600,"RetentionPeriodInDays":30}'
```

Pour supprimer la clé gérée par le client d'une fonction durable

Omettre `KMSKeyArn` de. `--durable-config` Les exécutions existantes continuent d'utiliser la clé gérée par le client avec laquelle elles ont commencé. Les nouvelles exécutions utilisent plutôt le chiffrement par défaut.

```
aws lambda update-function-configuration \
  --function-name myDurableFunction \
  --durable-config '{"ExecutionTimeout":3600,"RetentionPeriodInDays":30}'
```

AWS CloudFormation

Dans une `AWS::Lambda::Function` ressource, définissez la `KMSKeyArn` propriété de `DurableConfig` :

```
Resources:
  MyDurableFunction:
    Type: AWS::Lambda::Function
    Properties:
      FunctionName: myDurableFunction
      Runtime: nodejs24.x
      Handler: index.handler
      Role: !GetAtt MyDurableFunctionRole.Arn
      Code:
        ZipFile: |
          // Your durable function code
      DurableConfig:
        KMSKeyArn: "arn:aws:kms:us-east-1:111122223333:key/key-id"
        ExecutionTimeout: 3600
        RetentionPeriodInDays: 30
```

Important

Chaque exécution durable utilise la clé gérée par le client qui a été configurée sur la fonction lors de son démarrage. La modification ou la suppression de la clé n'affecte que les exécutions qui démarrent après la modification ; les exécutions en cours continuent d'utiliser la clé avec laquelle elles ont débuté jusqu'à ce qu'elles se terminent ou échouent.

Lecture de données d'exécution durables

Deux API de lecture renvoient des données d'exécution durables :

- `GetDurableExecution`renvoie l'état actuel d'une seule exécution, y compris sa charge utile d'entrée, les dernières données de point de contrôle et les informations relatives aux résultats ou aux erreurs.

- `GetDurableExecutionHistory`renvoie la liste ordonnée des événements émis par l'exécution, indiquant les entrées et les résultats des points de contrôle, les entrées et les résultats des appels en chaîne, ainsi que le résultat final.

Les deux API acceptent un paramètre de `IncludeExecutionData` requête. Dans `IncludeExecutionData` ce cas`true`, Lambda utilise les informations d'identification de l'appelant pour appeler la clé gérée par `kms:Decrypt` le client. Lambda renvoie ensuite les données d'exécution déchiffrées dans la réponse. L'identité de l'appelant doit figurer `kms:Decrypt` sur la clé gérée par le client.

Dans `IncludeExecutionData` ce cas`false`, Lambda n'appelle AWS KMS ni ne déchiffre les données d'exécution, et la réponse est définie sur. `ExecutionDataIncluded` `false` La réponse inclut toujours`DurableConfig`, ce qui fait écho à la clé ARN gérée par le client utilisée par l'exécution. `IncludeExecutionData`est défini par défaut sur`false`, de sorte que les appelants qui n'ont besoin que de métadonnées n'ont pas besoin d' AWS KMS autorisations.

Exemple : **`GetDurableExecution`** réponse avec **`IncludeExecutionData=false`**

```
{
    "DurableExecutionArn": "arn:aws:lambda:us-
east-1:111122223333:function:myDurableFunction:execution:exec-abc123",
    "DurableExecutionName": "exec-abc123",
    "FunctionArn": "arn:aws:lambda:us-east-1:111122223333:function:myDurableFunction",
    "StartTimestamp": 1733256000,
    "Status": "RUNNING",
    "ExecutionDataIncluded": false,
    "DurableConfig": {
        "ExecutionTimeout": 3600,
        "KMSKeyArn": "arn:aws:kms:us-east-1:111122223333:key/key-id",
        "RetentionPeriodInDays": 30
    }
}
```

Invoques enchaînées

Lorsqu'une fonction durable utilise un appel enchaîné pour appeler une autre fonction durable, Lambda traite l'exécution enfant comme une exécution durable indépendante : elle possède son propre identifiant d'exécution, son propre flux de points de contrôle et sa propre clé gérée par le client. La configuration des clés gérées par le client du parent n'a aucun effet sur les données de

l'enfant, et la configuration des clés gérées par le client de l'enfant n'a aucun effet sur les données du parent.

Permissions

Le responsable du service Lambda doit avoir `kms:GenerateDataKey` et `kms:Decrypt` sur la clé gérée par le client de la fonction enfant. Si les fonctions parent et enfant utilisent des clés gérées par le client différentes, vous accordez au principal du service l'accès à chaque clé séparément. Le rôle d'exécution de la fonction parent n'a pas besoin d'autorisations sur la clé gérée par le client de l'enfant.

Identifier quelle clé a chiffré quelle exécution

Les deux `GetDurableExecution` et `ListDurableExecutionsByFunction` renvoyez l'ARN de la clé gérée par le client qui a chiffré chaque exécution. Utilisez ces API pour vérifier quelle clé était active au début de l'exécution d'un parent ou d'un enfant.

Mise en cache des clés de données

Pour réduire le volume d' AWS KMS appels et améliorer la disponibilité en cas d'interruption de service, Lambda met en cache une clé de données générée à partir de votre clé gérée par le client pendant 15 minutes maximum. Lorsque le cache est chaud, Lambda réutilise la même clé de données entre les opérations d'une exécution et entre les exécutions démarrées pendant la fenêtre de cache.

Coût

Per-execution AWS KMS le coût reste faible car Lambda appelle `GenerateDataKey` au plus une fois par fenêtre de cache, et non une fois par point de contrôle. Lorsque les taux de demandes sont élevés, le coût par exécution diminue encore car un plus grand nombre d'exécutions partagent chaque clé de données mise en cache. Vous êtes facturé pour les AWS KMS appels que Lambda passe réellement, et non pour chaque point de contrôle ou chaque lecture.

Stabilité statique

Les clés de données restent en cache pendant 15 minutes maximum. Les modifications apportées à votre clé prennent effet lors de la prochaine actualisation du cache. Pendant les interruptions de service prolongées, Lambda continue de servir à partir du cache, ce qui permet de poursuivre les exécutions en cours.

CloudTrail

La mise en cache des clés de données signifie que vous voyez moins d'`GenerateDataKey`événements CloudTrail que d'exécutions ou de points de contrôle. Voir par Surveillance des clés KMS pour des fonctions durables exemple les événements.

Lorsque la clé gérée par le client n'est pas disponible

Si la clé gérée par le client avec laquelle une exécution a débuté est désactivée, si sa suppression est planifiée ou si son accès est révoqué par le biais de la politique des clés, l'exécution ne peut pas progresser davantage. Au point de contrôle suivant, Lambda échoue à l'exécution avec une AWS KMS erreur non réessayable. Le rétablissement de l'accès à la clé ne reprend pas automatiquement l'exécution. Vous devez lancer une nouvelle exécution.

Les API qui lisent ou écrivent des charges utiles échouent également lorsque la clé n'est pas disponible. Ils peuvent renvoyer l'une des exceptions suivantes :

- `KMSAccessDeniedException`: Lambda n'a pas pu déchiffrer les données d'exécution durables car l'accès à la clé KMS a été refusé.
- `KMSDisabledException`: Lambda n'a pas pu déchiffrer les données d'exécution durables car la clé KMS est désactivée.
- `KMSInvalidStateException`: Lambda n'a pas pu déchiffrer les données d'exécution durables car l'état de la clé KMS n'est pas valide pour. `Decrypt`
- `KMSNotFoundException`: Lambda n'a pas pu déchiffrer les données d'exécution durables car la clé KMS est introuvable.

La restauration de l'accès à la clé KMS permet à ces API de lecture de réussir à nouveau pour les exécutions qui ont déjà échoué. Les exécutions échouées restent des échecs ; vous devez recommencer une nouvelle exécution.

Pour inspecter les métadonnées d'exécution lorsque la clé KMS n'est pas disponible, appelez `GetDurableExecution` le`IncludeExecutionData=false`. Cela renvoie l'état de l'exécution, les horodatages et `DurableConfig` (y compris l'ARN de la clé KMS) sans appel. AWS KMS

Comme Lambda met en cache les clés de données, la désactivation d'une clé ne prend pas effet immédiatement. Pour plus de détails, consultez Mise en cache des clés de données.

> **Important**
>
> La suppression d'une clé KMS dont dépendent toujours les exécutions en cours ou conservées détruit définitivement ces exécutions et leur historique.

Surveillance des clés KMS pour des fonctions durables

Lorsque vous utilisez une clé gérée par le client dotée d'une fonction durable, vous pouvez l'utiliser AWS CloudTrailpour suivre les AWS KMS appels que Lambda passe en votre nom. Pour obtenir des conseils généraux sur les AWS KMS événements de recherche, consultez la section Activité des AWS KMS API de recherche.

Pour vérifier que Lambda utilise votre clé comme prévu, recherchez les champs suivants dans chaque événement :

- `eventName`: l'un des `GenerateDataKeyDecrypt`, ou `DescribeKey`
- `eventSource`: `kms.amazonaws.com`
- `userIdentity.invokedBy`: `lambda.amazonaws.com`
- `requestParameters.encryptionContext.aws:lambda:FunctionArn`: l'ARN de la fonction durable

Les exemples suivants sont CloudTrail des événements issus d'un `UpdateFunctionConfiguration` appel `CreateFunction` ou qui configure une clé gérée par le client sur une fonction durable. Lambda émet trois AWS KMS appels pour valider la clé : une clé réelle`DescribeKey`, une clé à sec `GenerateDataKey` et. `Decrypt`

GenerateDataKey

Lorsque vous définissez ou modifiez l'entrée`DurableConfig`, Lambda émet une analyse `KMSKeyArn` à sec `GenerateDataKey` sur la clé gérée par le client pour valider que la politique en matière de clés permet à Lambda de dériver des clés de données pour le contexte de chiffrement de cette fonction. Le dry-run n'effectue aucun travail cryptographique mais enregistre un événement complet. CloudTrail L'exemple d'événement suivant enregistre l'opération de séchage : `GenerateDataKey`

```
{
    "eventVersion": "1.11",
```

```
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROA123456789EXAMPLE:example",
        "arn": "arn:aws:sts::111122223333:assumed-role/FunctionAuthor/example",
        "accountId": "111122223333",
        "accessKeyId": "ASIA123456789EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROA123456789EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/FunctionAuthor",
                "accountId": "111122223333",
                "userName": "FunctionAuthor"
            },
            "attributes": {
                "creationDate": "2026-01-15T16:54:42Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "lambda.amazonaws.com"
    },
    "eventTime": "2026-01-15T16:55:00Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "lambda.amazonaws.com",
    "userAgent": "lambda.amazonaws.com",
    "errorCode": "DryRunOperationException",
    "errorMessage": "The request would have succeeded, but the DryRun option is
 set.",
    "requestParameters": {
        "encryptionContext": {
            "aws:lambda:FunctionArn": "arn:aws:lambda:us-
east-1:111122223333:function:myDurableFunction"
        },
        "dryRun": true,
        "keyId": "arn:aws:kms:us-east-1:111122223333:key/key-id",
        "keySpec": "AES_256"
    },
    "responseElements": null,
    "additionalEventData": {
        "keyMaterialId":
 "a1b2c3d4e5f6a7b8c9d0e1f2a3b4c5d6e7f8a9b0c1d2e3f4a5b6c7d8e9f0EXAMPLE"
    },
```

```
    "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa",
    "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLEbbbbb",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-east-1:111122223333:key/key-id"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Decrypt

Lorsque vous définissez ou modifiez l'entrée`DurableConfig`, Lambda émet également un essai `KMSKeyArn` à sec sur la clé gérée par le client pour valider que la politique de clé autorise Lambda à déchiffrer les données pour le `Decrypt` contexte de chiffrement de cette fonction. Le dry-run utilise`IGNORE_CIPHERTEXT`, donc aucun véritable texte chiffré n'est requis. L'exemple d'événement suivant enregistre l'opération de séchage : `Decrypt`

```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROA123456789EXAMPLE:example",
        "arn": "arn:aws:sts::111122223333:assumed-role/FunctionAuthor/example",
        "accountId": "111122223333",
        "accessKeyId": "ASIA123456789EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROA123456789EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/FunctionAuthor",
                "accountId": "111122223333",
                "userName": "FunctionAuthor"
            },
            "attributes": {
                "creationDate": "2026-01-15T16:54:42Z",
                "mfaAuthenticated": "false"
```

```
            }
        },
        "invokedBy": "lambda.amazonaws.com"
    },
    "eventTime": "2026-01-15T16:55:00Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "lambda.amazonaws.com",
    "userAgent": "lambda.amazonaws.com",
    "errorCode": "DryRunOperationException",
    "errorMessage": "The request would have succeeded, but the DryRun option is
 set.",
    "requestParameters": {
        "encryptionContext": {
            "aws:lambda:FunctionArn": "arn:aws:lambda:us-
east-1:111122223333:function:myDurableFunction"
        },
        "dryRun": true,
        "keyId": "arn:aws:kms:us-east-1:111122223333:key/key-id",
        "dryRunModifiers": ["IGNORE_CIPHERTEXT"],
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
    },
    "responseElements": null,
    "additionalEventData": {
        "keyMaterialId":
 "a1b2c3d4e5f6a7b8c9d0e1f2a3b4c5d6e7f8a9b0c1d2e3f4a5b6c7d8e9f0EXAMPLE"
    },
    "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa",
    "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLEbbbbb",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-east-1:111122223333:key/key-id"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

DescribeKey

Lorsque vous définissez ou modifiez l'entrée `KMSKeyArnDurableConfig`, Lambda appelle `DescribeKey` pour confirmer que la clé est symétrique et activée avant d'accepter la modification. Contrairement aux `Decrypt` sondes `GenerateDataKey` et, il s'agit d'un véritable appel, et non d'un essai à sec. L'exemple d'événement suivant enregistre l'opération `DescribeKey` :


```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROA123456789EXAMPLE:example",
        "arn": "arn:aws:sts::111122223333:assumed-role/FunctionAuthor/example",
        "accountId": "111122223333",
        "accessKeyId": "ASIA123456789EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROA123456789EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/FunctionAuthor",
                "accountId": "111122223333",
                "userName": "FunctionAuthor"
            },
            "attributes": {
                "creationDate": "2026-01-15T16:54:42Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "lambda.amazonaws.com"
    },
    "eventTime": "2026-01-15T16:55:00Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DescribeKey",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "lambda.amazonaws.com",
    "userAgent": "lambda.amazonaws.com",
    "requestParameters": {
        "keyId": "arn:aws:kms:us-east-1:111122223333:key/key-id"
    },
    "responseElements": null,
    "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa",
    "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLEbbbbb",
```

```
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-east-1:111122223333:key/key-id"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Sujets de chiffrement connexes

- Chiffrement des données au repos pour Lambda
- Sécurisation des variables d'environnement Lambda
- Chiffrement des packages de déploiement Lambda .zip
- Modèle de sécurité pour Lambda SnapStart
- Configurer les fonctions durables de Lambda

SDK d'exécution durable

Le SDK d'exécution durable constitue la base de la création de fonctions durables. Il fournit des primitives pour contrôler la progression des points, gérer les nouvelles tentatives et gérer le flux d'exécution. Le SDK résume la complexité de la gestion et de la réexécution des points de contrôle, vous permettant d'écrire du code séquentiel qui devient automatiquement tolérant aux pannes.

Le SDK est disponible pour JavaScript, TypeScript, Python, Java, Go et C# (.NET). Pour une documentation complète sur l'API, des didacticiels de démarrage rapide et des guides spécifiques à chaque langue, consultez le AWS Guide du développeur du SDK Durable Execution.

Ce que fait le SDK

Gestion des points de contrôle : Le SDK crée automatiquement des points de contrôle lorsque votre fonction exécute des opérations durables. Chaque point de contrôle enregistre le type d'opération, les entrées et les résultats. Lorsque votre fonction termine une étape, le SDK maintient le point de

contrôle avant de continuer. Cela garantit que votre fonction peut reprendre après une opération terminée en cas d'interruption.

Coordination des rediffusions : Lorsque votre fonction reprend après une pause ou une interruption, le SDK effectue une relecture. Il exécute votre code depuis le début mais ignore les opérations terminées, en utilisant les résultats des points de contrôle enregistrés au lieu de les réexécuter. Le SDK garantit que la rediffusion est déterministe. Avec les mêmes entrées et le même journal de points de contrôle, votre fonction produit les mêmes résultats.

Isolement de l'État : Le SDK gère l'état d'exécution séparément de votre logique métier. Chaque exécution durable possède son propre journal des points de contrôle auquel les autres exécutions ne peuvent pas accéder. Le SDK chiffre les données des points de contrôle au repos et garantit que l'état reste cohérent entre les rediffusions.

Pour une explication détaillée du fonctionnement du point de contrôle et du comportement des rediffusions, voir Concepts clés dans le AWS Guide du développeur du SDK Durable Execution.

Opérations durables

Le SDK fournit à votre fonction un `DurableContext` objet. Ce contexte remplace le contexte Lambda standard et fournit des méthodes pour créer des points de contrôle, gérer le flux d'exécution et coordonner avec des systèmes externes.

Le `DurableContext` fournit les opérations suivantes pour créer des flux de travail durables :

Opération	Description
Step (Étape)	Exécutez et contrôlez une unité de travail à l'aide de stratégies de nouvelle tentative configurables et d'une sémantique d'exécution.
Attente	Suspendez l'exécution pendant une durée spécifiée sans consommer de ressources de calcul.
Attendre la condition	Sondage pour une condition avec un point de contrôle automatique entre les tentatives.
Rappel	Suspendez l'exécution et attendez qu'un système externe fournisse des données via l'API Lambda.

Opération	Description
Invoke	Appelez une autre fonction Lambda et attendez son résultat, avec un point de contrôle automatique.
Parallèle	Exécutez plusieurs opérations simultanément grâce à des politiques d'achèvement configurables.
Map	Traitez chaque élément d'une collection simultanément grâce au contrôle de simultanéité facultatif.
Contexte de l'enfant	Créez un contexte d'exécution isolé pour regrouper plusieurs opérations.

Chaque opération durable crée automatiquement des points de contrôle, garantissant ainsi la reprise de votre activité à tout moment. Pour une référence détaillée de l'API, des exemples de code et une utilisation spécifique au langage, voir Référence du SDK dans le AWS Guide du développeur du SDK Durable Execution.

Comment les opérations durables sont-elles mesurées

Chaque opération durable par laquelle vous appelez `DurableContext` crée des points de contrôle pour suivre la progression de l'exécution et stocker les données d'état. Ces opérations sont payantes en fonction de leur utilisation, et les points de contrôle peuvent contenir des données qui contribuent à vos coûts d'écriture et de conservation des données. Les données stockées incluent les données relatives aux événements d'invocation, les charges utiles renvoyées par les étapes et les données transmises lors de l'exécution des rappels. Comprendre comment les opérations durables sont mesurées vous permet d'estimer les coûts d'exécution et d'optimiser vos flux de travail. Pour plus de détails sur les tarifs, consultez le Page de tarification Lambda.

La taille de la charge utile fait référence à la taille des données sérialisées qu'une opération durable persiste. Les données sont mesurées en octets et leur taille peut varier en fonction du sérialiseur utilisé par l'opération. La charge utile d'une opération peut être le résultat lui-même en cas d'achèvement réussi, ou l'objet d'erreur sérialisé si l'opération a échoué.

Opérations de base

Les opérations de base sont les éléments fondamentaux des fonctions durables :

Opération	Calendrier des points de contrôle	Nombre d'opérations	Les données ont persisté
Exécution	Démarré(e)	1	Taille de la charge utile d'entrée
Exécution	Terminé (Succeeded/Failed/Stopped)	0	Taille de la charge utile de sortie
Step (Étape)	Retry/Succeeded/Failed	1 + Aucune tentative	Taille de la charge utile renvoyée à chaque tentative
Attente	Démarré(e)	1	N/A
WaitForCondition	Chaque tentative de sondage	1 + N sondages	Taille de la charge utile renvoyée à chaque tentative de sondage
Invocation-level Réessayez	Démarré(e)	1	Charge utile pour l'objet d'erreur

Opérations de rappel

Les opérations de rappel permettent à votre fonction de faire une pause et d'attendre que les systèmes externes fournissent une entrée. Ces opérations créent des points de contrôle lorsque le rappel est créé et lorsqu'il est terminé :

Opération	Calendrier des points de contrôle	Nombre d'opérations	Les données ont persisté
CreateCallback	Démarré(e)	1	N/A
Exécution du rappel via un appel d'API	Terminé	0	Charge utile de rappel
WaitForCallback	Démarré(e)	3 + N tentatives	Charges utiles renvoyées par les tentatives d'étape de l'expéditeur,

Opération	Calendrier des points de contrôle	Nombre d'opérations	Les données ont persisté
		(contexte + rappel + étape)	plus deux copies de la charge utile de rappel

Opérations composées

Les opérations composées combinent plusieurs opérations durables pour gérer des modèles de coordination complexes tels que l'exécution parallèle, le traitement de tableaux et les contextes imbriqués :

Opération	Calendrier des points de contrôle	Nombre d'opérations	Les données ont persisté
Parallèle	Démarré(e)	1 + N branches (1 contexte parent + N contextes enfant)	Jusqu'à deux copies de la taille de la charge utile renvoyée par chaque branche, plus les statuts de chaque branche
Map	Démarré(e)	1 + N branches (1 contexte parent + N contextes enfant)	Jusqu'à deux copies de la taille de la charge utile renvoyée pour chaque itération, plus les statuts de chaque itération

Opération	Calendrier des points de contrôle	Nombre d'opérations	Les données ont persisté
Promise helpers	Terminé	1	Taille de la charge utile renvoyée à partir de la promesse
RunInChildContext	Succeeded/Failed	1	Taille de la charge utile renvoyée depuis le contexte de l'enfant

Pour des contextes tels que `runInChildContext` ou utilisés en interne par des opérations composées, les résultats inférieurs à 256 Ko sont vérifiés directement. Les résultats plus volumineux ne sont pas stockés, mais reconstruits lors de la rediffusion en retraitant les opérations du contexte.

Runtimes pris en charge pour des fonctions durables

Des fonctions durables sont disponibles pour certains environnements d'exécution gérés et les images de conteneurs OCI pour une flexibilité accrue des versions d'exécution. Vous pouvez créer des fonctions durables pour Python Node.js, Java et C# (.NET) en utilisant des environnements d'exécution gérés directement dans la console ou par programmation via l'infrastructure en tant que code.

Runtimes gérés par Lambda

Les environnements d'exécution gérés suivants prennent en charge les fonctions durables lorsque vous créez des fonctions dans la console Lambda ou que vous utilisez le AWS CLI `--durable-config '{"ExecutionTimeout": 3600, "RetentionPeriodInDays": 7}'` paramètre with. Pour des informations complètes sur les environnements d'exécution Lambda, consultez la section Runtimes Lambda.

Language	Environnement d’exécution
Node.js	nodejs22.x
Node.js	nodejs24.x
Python	python 3.13

Language	Environnement d’exécution
Python	python 3.14
Java	java17
Java	java21
Java	java25
C# (.NET)	dotnet 8
C# (.NET)	dotnet10

> **Note**
>
> Les environnements d'exécution Lambda Node.js et Python incluent le SDK d'exécution durable pour les tests et le développement. Nous vous recommandons toutefois d'inclure le SDK dans votre package de déploiement pour la production. Cela garantit la cohérence des versions et évite les éventuelles mises à jour d'exécution qui pourraient affecter le comportement de votre fonction. Java et C# (.NET) étant des langages compilés, les environnements d'exécution Lambda Java et .NET n'incluent pas le SDK d'exécution durable. Il doit donc être inclus dans votre package de déploiement.

Node.js

Installez le SDK dans votre Node.js projet :

```
npm install @aws/durable-execution-sdk-js
```

Le SDK prend en charge JavaScript et. TypeScript Pour les TypeScript projets, le SDK inclut des définitions de type.

Python

Installez le SDK dans votre projet Python :

```
pip install aws-durable-execution-sdk-python
```

Le SDK Python utilise des méthodes synchrones et n'en a pas besoin. `async/await`

Java

Ajoutez une dépendance à `pom.xml` :

```
<dependency>
    <groupId>software.amazon.lambda.durable</groupId>
    <artifactId>aws-durable-execution-sdk-java</artifactId>
    <version>VERSION</version>
</dependency>
```

Installez le SDK dans votre projet Java :

```
mvn install
```

Le SDK Java fournit des versions synchrones et asynchrones de chaque méthode.

C# (.NET)

Ajoutez le SDK à votre projet .NET :

```
dotnet add package Amazon.Lambda.DurableExecution
```

Le SDK .NET expose les opérations durables via. `IDurableContext` Votre gestionnaire reçoit l'enveloppe de service d'exécution durable et délègue à`DurableFunction.WrapAsync`. Chaque corps d'opération prend un`CancellationToken`.

Images de conteneurs

Vous pouvez utiliser des fonctions durables avec des images de conteneur pour prendre en charge des versions d'exécution supplémentaires ou des configurations d'exécution personnalisées. Les

images de conteneur vous permettent d'utiliser des versions d'exécution non disponibles en tant que moteurs d'exécution gérés ou de personnaliser votre environnement d'exécution.

Pour créer une fonction durable à l'aide d'une image de conteneur :

1. Créer un Dockerfile basé sur une image de base Lambda
2. Installez le SDK d'exécution durable dans votre conteneur
3. Créez et transférez l'image du conteneur vers Amazon Elastic Container Registry
4. Créez la fonction Lambda à partir de l'image du conteneur avec l'exécution durable activée

Exemple de conteneur

Créez un Dockerfile :

Python

Créez un Dockerfile pour Python 3.11 :

```
FROM public.ecr.aws/lambda/python:3.11

# Copy requirements file
COPY requirements.txt ${LAMBDA_TASK_ROOT}/

# Install dependencies including durable SDK
RUN pip install -r requirements.txt

# Copy function code
COPY lambda_function.py ${LAMBDA_TASK_ROOT}/

# Set the handler
CMD [ "lambda_function.handler" ]
```

Créez un `requirements.txt` fichier :

```
aws-durable-execution-sdk-python
```

Java

Créez un Dockerfile pour Java 25 :

```
FROM --platform=linux/amd64 public.ecr.aws/lambda/java:25

# Install Maven
RUN dnf install -y maven

WORKDIR /var/task

# Copy Maven configuration and source code
COPY pom.xml .
COPY src ./src

# Build
RUN mvn clean package -DskipTests

# Move JAR to lib directory
RUN mv target/*.jar lib/

# Set the handler
CMD ["src.path.to.lambdaFunction::handler"]
```

Créez et diffusez l'image :

```
# Build the image
docker build -t my-durable-function .

# Tag for ECR
docker tag my-durable-function:latest 123456789012.dkr.ecr.us-east-1.amazonaws.com/my-
durable-function:latest

# Push to ECR
docker push 123456789012.dkr.ecr.us-east-1.amazonaws.com/my-durable-function:latest
```

Créez la fonction avec l'exécution durable activée :

```
aws lambda create-function \
  --function-name myDurableFunction \
  --package-type Image \
  --code ImageUri=123456789012.dkr.ecr.us-east-1.amazonaws.com/my-durable-
function:latest \
  --role arn:aws:iam::123456789012:role/lambda-execution-role \
  --durable-config '{"ExecutionTimeout": 3600, "RetentionPeriodInDays": 7}'
```

Pour plus d'informations sur l'utilisation d'images de conteneur avec Lambda, consultez la section Création d'images de conteneur Lambda dans le Lambda Developer Guide.

Considérations relatives à l’exécution

Gestion des versions du SDK : pour conserver le contrôle total de vos dépendances et éviter d'éventuels problèmes de désalignement des versions, nous vous recommandons d'ajouter toutes les dépendances de votre fonction à votre package de déploiement, même si des versions de celles-ci sont incluses par défaut dans le runtime Lambda. Cela inclut le SDK d'exécution durable. Verrouillez le SDK d'exécution durable sur une version majeure dans votre fichier de dépendances. Une nouvelle version majeure peut introduire des modifications susceptibles d'entraîner l'échec des exécutions en vol. Utilisez des versions numérotées ou des alias pour les fonctions durables de production plutôt que pour `$LATEST` vous assurer que les modifications de version du SDK n'affectent pas les exécutions en cours.

Mises à jour d'exécution : AWS met à jour les environnements d'exécution gérés pour inclure des correctifs de sécurité et des corrections de bogues. Ces mises à jour peuvent inclure de nouvelles versions du SDK. Pour éviter tout comportement inattendu, incluez le SDK dans votre package de déploiement et testez-le minutieusement avant le déploiement en production.

Taille de l'image de conteneur : les images de conteneur ont une taille non compressée maximale de 10 Go. Le SDK d'exécution durable ajoute une taille minimale à votre image. Optimisez votre conteneur en utilisant des versions en plusieurs étapes et en supprimant les dépendances inutiles.

Performances de démarrage à froid : les temps de démarrage à froid des images de conteneurs peuvent être plus longs que ceux des environnements d'exécution gérés. Le SDK d'exécution durable a un impact minimal sur les performances de démarrage à froid. Utilisez la simultanéité provisionnée si la latence de démarrage à froid est essentielle pour votre application.

Invoquer les fonctions durables de Lambda

Les fonctions Lambda durables prennent en charge les mêmes méthodes d'appel que les autres fonctions Lambda. Vous pouvez appeler des fonctions durables de manière synchrone, asynchrone ou via des mappages de sources d'événements. Le processus d'invocation est identique aux autres fonctions, mais les fonctions durables offrent des fonctionnalités supplémentaires pour les exécutions de longue durée et la gestion automatique des états.

Méthodes d'invocation

Invocation synchrone : invoquez une fonction durable et attendez la réponse. Les appels synchrones sont limités à 15 minutes, ou moins si le délai d'expiration de la fonction ou le délai d'exécution est inférieur. Utilisez l'invocation synchrone lorsque vous avez besoin de résultats immédiats ou lorsque vous intégrez des API et des services qui attendent une réponse. Vous pouvez utiliser les opérations d'attente pour un calcul efficace sans perturber l'appelant : l'invocation attend la fin de l'exécution durable complète. Pour les démarrages d'exécution idempotents, utilisez le paramètre de nom d'exécution tel que décrit dans Idempotentie.

```
aws lambda invoke \
  --function-name my-durable-function:1 \
  --cli-binary-format raw-in-base64-out \
  --payload '{"orderId": "12345"}' \
  response.json
```

Invocation asynchrone : mettez en file d'attente un événement pour qu'il soit traité sans attendre de réponse. Lambda place l'événement dans une file d'attente et y retourne immédiatement. Les invocations asynchrones prennent en charge des durées d'exécution allant jusqu'à 1 an. Utilisez l'invocation asynchrone pour les scénarios « fire and forget » ou lorsque le traitement peut se faire en arrière-plan. Pour les démarrages d'exécution idempotents, utilisez le paramètre de nom d'exécution tel que décrit dans Idempotentie.

```
aws lambda invoke \
  --function-name my-durable-function:1 \
  --invocation-type Event \
  --cli-binary-format raw-in-base64-out \
  --payload '{"orderId": "12345"}' \
  response.json
```

Mappages de sources d'événements : configurez Lambda pour appeler automatiquement votre fonction durable lorsque des enregistrements sont disponibles à partir de services basés sur des flux ou des files d'attente tels qu'Amazon SQS, Kinesis ou DynamoDB. Les mappages de sources d'événements interrogent la source d'événements et invoquent votre fonction avec des lots d'enregistrements. Pour plus de détails sur l'utilisation des mappages de sources d'événements avec des fonctions durables, y compris les limites de durée d'exécution, voir Mappages de sources d'événements avec des fonctions durables.

Pour obtenir des informations complètes sur chaque méthode d'appel, consultez les sections Invocation synchrone et Invocation asynchrone.

> **Note**
>
> Les fonctions durables prennent en charge les files d'attente en lettres mortes (DLQ) pour la gestion des erreurs, mais ne prennent pas en charge les destinations Lambda. Configurez un DLQ pour capturer les enregistrements des appels ayant échoué.

Exigence d'ARN qualifiés

Les fonctions durables nécessitent des identifiants qualifiés pour l'invocation. Vous devez invoquer des fonctions durables à l'aide d'un numéro de version, d'un alias ou`$LATEST`. Vous pouvez utiliser un ARN qualifié complet ou un nom de fonction avec version/alias suffixe. Vous ne pouvez pas utiliser un identifiant non qualifié (sans version ni suffixe d'alias).

Invocations valides :

```
# Using full ARN with version number
arn:aws:lambda:us-east-1:123456789012:function:my-durable-function:1

# Using full ARN with alias
arn:aws:lambda:us-east-1:123456789012:function:my-durable-function:prod

# Using full ARN with $LATEST
arn:aws:lambda:us-east-1:123456789012:function:my-durable-function:$LATEST

# Using function name with version number
```

```
my-durable-function:1

# Using function name with alias
my-durable-function:prod
```

Invocations non valides :

```
# Unqualified ARN (not allowed)
arn:aws:lambda:us-east-1:123456789012:function:my-durable-function

# Unqualified function name (not allowed)
my-durable-function
```

Cette exigence garantit que les exécutions durables restent cohérentes tout au long de leur cycle de vie. Lorsqu'une exécution durable démarre, elle est épinglée à la version de la fonction qui l'a lancée. Si votre fonction s'arrête et reprend des heures ou des jours plus tard, Lambda invoque la même version. La publication d'une nouvelle version n'affecte donc que les nouvelles exécutions. De même, lorsque vous mettez à jour un alias, les nouvelles exécutions utilisent la nouvelle version et les exécutions en cours se poursuivent sur la version sur laquelle elles ont débuté.

⚠ **Les exécutions de `$LATEST`** peuvent reprendre sur le code mis à jour

Les exécutions démarrées avec le `$LATEST` qualificatif ne sont pas associées à une copie fixe de votre code. Si vous mettez à jour votre code de fonction alors qu'une exécution est suspendue, l'exécution reprend sur le nouveau code plutôt que sur la version sur laquelle elle a débuté.

Il est possible que votre code ne traite plus l'état d'exécution enregistré de la même manière, ce qui entraîne des erreurs non déterministes ou des échecs silencieux. Pour plus d'informations sur l'écriture de fonctions qui se rejouent en toute sécurité, consultezVersions et alias des fonctions.

Bonne pratique

Utilisez plutôt `$LATEST` des versions numérotées ou des alias pour produire des fonctions durables. Les versions numérotées sont immuables et permettent une rediffusion déterministe. Les alias

fournissent éventuellement une référence stable que vous pouvez mettre à jour pour pointer vers de nouvelles versions sans modifier le code d'appel. À utiliser `$LATEST` uniquement pour le prototypage ou pour raccourcir les délais de déploiement pendant le développement, car les exécutions risquent de ne pas être reexécutées correctement si le code change pendant leur exécution.

Comprendre le cycle de vie d'exécution

Lorsque vous appelez une fonction durable, Lambda crée une exécution durable qui peut couvrir plusieurs invocations de fonction :

1. Invocation initiale : votre demande d'invocation crée une nouvelle exécution durable. Lambda attribue un ID d'exécution unique et lance le traitement.
2. Exécution et pointage : lorsque votre fonction exécute des opérations durables, le SDK crée des points de contrôle qui permettent de suivre la progression.
3. Suspension (si nécessaire) : si votre fonction utilise des temps d'attente prolongés, tels que `wait` des tentatives ou des tentatives automatiques`waitForCallback`, Lambda suspend l'exécution et arrête de facturer le temps de calcul.
4. Reprise : au moment de reprendre (y compris après de nouvelles tentatives), Lambda invoque à nouveau votre fonction. Le SDK rejoue le journal des points de contrôle et continue à partir de l'endroit où l'exécution a été interrompue.
5. Achèvement : lorsque votre fonction renvoie un résultat final ou renvoie une erreur non gérée, l'exécution durable est terminée.

Pour les invocations synchrones, l'appelant attend la fin complète de l'exécution durable, y compris les opérations d'attente. Si l'exécution dépasse le délai d'invocation (15 minutes ou moins), l'invocation expire. Pour les invocations asynchrones, Lambda revient immédiatement et l'exécution se poursuit indépendamment. Utilisez les API d'exécution durable pour suivre l'état d'exécution et obtenir les résultats finaux.

Invocation depuis le code de l'application

Utilisez les AWS SDK pour invoquer des fonctions durables à partir du code de votre application, avec la même `Invoke` API que celle que vous utilisez pour n'importe quelle fonction Lambda. Incluez un numéro de version, un alias ou `$LATEST` dans le nom de la fonction :

TypeScript

```
import { LambdaClient, InvokeCommand } from '@aws-sdk/client-lambda';

const client = new LambdaClient({});

// Synchronous invocation
const response = await client.send(new InvokeCommand({
  FunctionName: 'arn:aws:lambda:us-east-1:123456789012:function:my-durable-
function:1',
  Payload: JSON.stringify({ orderId: '12345' })
}));

const result = JSON.parse(Buffer.from(response.Payload!).toString());

// Asynchronous invocation
await client.send(new InvokeCommand({
  FunctionName: 'arn:aws:lambda:us-east-1:123456789012:function:my-durable-
function:1',
  InvocationType: 'Event',
  Payload: JSON.stringify({ orderId: '12345' })
}));
```

Python

```
import boto3
import json

client = boto3.client('lambda')

# Synchronous invocation
response = client.invoke(
    FunctionName='arn:aws:lambda:us-east-1:123456789012:function:my-durable-
function:1',
    Payload=json.dumps({'orderId': '12345'})
)

result = json.loads(response['Payload'].read())

# Asynchronous invocation
client.invoke(
    FunctionName='arn:aws:lambda:us-east-1:123456789012:function:my-durable-
function:1',
```

```
    InvocationType='Event',
    Payload=json.dumps({'orderId': '12345'})
)
```

Invocations enchaînées

Les fonctions durables peuvent appeler n'importe quelle fonction Lambda, y compris une autre fonction durable, en utilisant l'`invoke`opération from. `DurableContext` Cela crée un appel enchaîné où la fonction appelante est suspendue jusqu'à ce que la fonction invoquée soit terminée :

TypeScript

```
export const handler = withDurableExecution(
  async (event: any, context: DurableContext) => {
    // Invoke another durable function and wait for result
    const result = await context.invoke(
      'process-order',
      'arn:aws:lambda:us-east-1:123456789012:function:order-processor:1',
      { orderId: event.orderId }
    );

    return { statusCode: 200, body: JSON.stringify(result) };
  }
);
```

Python

```
@durable_execution
def handler(event, context: DurableContext):
    # Invoke another durable function and wait for result
    result = context.invoke(
        'arn:aws:lambda:us-east-1:123456789012:function:order-processor:1',
        {'orderId': event['orderId']},
        name='process-order'
    )

    return {'statusCode': 200, 'body': json.dumps(result)}
```

Les invocations enchaînées créent un point de contrôle dans la fonction d'appel. Si la fonction appelante est interrompue, elle repart du point de contrôle avec le résultat de la fonction invoquée, sans la réinvoquer.

> **Note**
>
> Cross-account les invocations enchaînées ne sont pas prises en charge. La fonction invoquée doit se trouver dans le même AWS compte que la fonction appelante.

Mappages de sources d'événements dotés de fonctions durables

Les fonctions durables fonctionnent avec tous les mappages de sources d'événements Lambda. Configurez les mappages de sources d'événements pour les fonctions durables de la même manière que vous les configurez pour les autres fonctions. Les mappages de sources d'événements interrogent automatiquement des sources d'événements telles qu'Amazon SQS, Kinesis et DynamoDB Streams, et invoquent votre fonction à l'aide de lots d'enregistrements.

Les mappages de sources d'événements sont utiles pour les fonctions durables qui traitent des flux ou des files d'attente avec des flux de travail complexes en plusieurs étapes. Par exemple, vous pouvez créer une fonction durable qui traite les messages Amazon SQS avec de nouvelles tentatives, des appels d'API externes et des approbations humaines.

Comment les mappages de sources d'événements invoquent des fonctions durables

Les mappages de sources d'événements invoquent des fonctions durables de manière synchrone, en attendant la fin de l'exécution durable complète avant de traiter le lot suivant ou de marquer les enregistrements comme traités. Si le temps d'exécution durable total dépasse le délai d'expiration applicable (15 minutes par défaut, ou jusqu'à 90 minutes pour les fonctions exécutées sur des instances gérées Lambda), l'exécution expire et échoue. Le mappage de la source d'événements reçoit une exception de délai d'attente et la gère en fonction de sa configuration de nouvelle tentative.

Limite de durée d'exécution

Lorsque des fonctions durables sont invoquées par des mappages de sources d'événements, la durée totale d'exécution durable ne peut pas dépasser le délai d'expiration maximal des fonctions : 15

minutes pour les fonctions exécutées en mode de capacité par défaut (à la demande), ou jusqu'à 90 minutes pour les fonctions exécutées sur des instances gérées Lambda (à l'exception des mappages de sources d'événements Amazon MQ et Amazon DocumentDB, qui restent limités à 15 minutes). Cette limite s'applique à l'ensemble de l'exécution durable, du début à la fin, et pas uniquement aux invocations de fonctions individuelles.

Le délai d'expiration de la fonction limite chaque appel. Le délai d'exécution durable limite le temps total entre le début et la fin de l'exécution. Avec les mappages de sources d'événements, les deux ont le même maximum : 15 minutes par défaut, ou 90 minutes sur les instances gérées Lambda.

Exemples de scénarios :

- Valide (n'importe quel mode de capacité) : une fonction durable traite un message Amazon SQS en trois étapes, chacune prenant 2 minutes, puis attend 5 minutes avant de terminer une étape finale. Durée totale d'exécution : 11 minutes Cela fonctionne sur les deux modes de capacité car la limite par défaut de 15 minutes est inférieure à la limite par défaut.
- Valable uniquement sur les instances gérées Lambda : une fonction durable traite un message Amazon SQS, effectue le traitement initial en 2 minutes, puis attend 20 minutes pour un rappel externe avant de terminer. Durée totale d'exécution : 22 minutes. Cela dépasse la limite par défaut de 15 minutes, mais se situe dans la limite de 90 minutes pour les fonctions exécutées sur des instances gérées Lambda.
- Non valide (quel que soit le mode de capacité) : une fonction durable traite un enregistrement Kinesis avec plusieurs opérations d'attente d'un total de deux heures entre les étapes. Cela dépasse même la limite de 90 minutes pour les instances gérées Lambda, de sorte que l'exécution échoue quel que soit le mode de capacité. Utilisez le modèle de fonction intermédiaire pour les flux de travail de cette longueur.

> **Important**
>
> Configurez votre délai d'exécution durable dans les limites applicables lorsque vous utilisez des mappages de sources d'événements ou si la création du mappage de source d'événements échoue. La limite est de 15 minutes par défaut, ou jusqu'à 90 minutes sur les instances gérées Lambda. Si votre flux de travail nécessite des temps d'exécution plus longs, utilisez le modèle de fonction intermédiaire décrit ci-dessous.

Configuration des mappages de sources d'événements

Configurez les mappages de sources d'événements pour des fonctions durables à l'aide de la console Lambda ou AWS CLI des SDK. AWS Toutes les propriétés de mappage des sources d'événements, telles que la taille du lot et la fenêtre de traitement par lots, s'appliquent aux fonctions durables :

```
aws lambda create-event-source-mapping \
  --function-name arn:aws:lambda:us-east-1:123456789012:function:my-durable-function:1
 \
  --event-source-arn arn:aws:sqs:us-east-1:123456789012:my-queue \
  --batch-size 10 \
  --maximum-batching-window-in-seconds 5
```

Utilisez un ARN qualifié avec un numéro de version, un alias ou `$LATEST` lorsque vous configurez un mappage de source d'événements pour une fonction durable.

Gestion des erreurs avec les mappages de sources d'événements

Les mappages de sources d'événements fournissent une gestion des erreurs intégrée qui fonctionne avec des fonctions durables :

- Comportement de nouvelle tentative : si l'appel initial échoue, le mappage de la source d'événements réessaie conformément à sa configuration de nouvelle tentative. Configurez le nombre maximal de tentatives et les intervalles entre les tentatives en fonction de vos besoins.
- Dead-letter files d'attente : configurez une file d'attente contenant des lettres mortes pour capturer les enregistrements qui échouent après chaque nouvelle tentative. Cela empêche la perte de messages et permet une inspection manuelle des enregistrements défaillants.
- Défaillances partielles par lots : pour Amazon SQS et Kinesis, utilisez le rapport d'échec partiel des lots pour traiter les enregistrements individuellement et réessayez uniquement les enregistrements ayant échoué.
- Couper en deux en cas d'erreur : pour Kinesis et DynamoDB Streams, activez la division en deux en cas d'erreur pour diviser les lots ayant échoué et isoler les enregistrements problématiques.

> **Note**
>
> Les fonctions durables prennent en charge les files d'attente en lettres mortes (DLQ) pour la gestion des erreurs, mais ne prennent pas en charge les destinations Lambda. Configurez un DLQ pour capturer les enregistrements des appels ayant échoué.

Pour des informations complètes sur la gestion des erreurs de mappage des sources d'événements, consultez la section Mappages des sources d'événements.

Utilisation d'une fonction intermédiaire pour les flux de travail de longue durée

Si votre flux de travail nécessite plus que la limite de mappage des sources d'événements applicable (15 minutes par défaut, ou 90 minutes sur les instances gérées Lambda), utilisez une fonction Lambda standard intermédiaire entre le mappage des sources d'événements et votre fonction durable. La fonction intermédiaire reçoit les événements du mappage de la source d'événements et invoque la fonction durable de manière asynchrone, supprimant ainsi la limite de durée d'exécution.

Ce modèle dissocie le modèle d'appel synchrone du mappage des sources d'événements du modèle d'exécution à long terme de la fonction durable. Le mappage de la source d'événements invoque la fonction intermédiaire, qui revient rapidement après le démarrage de l'exécution durable. La fonction durable fonctionne ensuite de manière indépendante aussi longtemps que nécessaire (jusqu'à 1 an).

Architecture

Le modèle de fonction intermédiaire utilise trois composants :

1. Cartographie de la source d'événements : interroge la source de l'événement (Amazon SQS, Kinesis, DynamoDB Streams) et invoque la fonction intermédiaire de manière synchrone avec des lots d'enregistrements.
2. Fonction intermédiaire : fonction Lambda sans exécution durable qui reçoit des événements provenant du mappage de la source d'événements, valide et transforme les données si nécessaire, et invoque la fonction durable de manière asynchrone. Cette fonction s'exécute rapidement (généralement en moins d'une seconde) et redonne le contrôle au mappage des sources d'événements.
3. Fonction durable : traite l'événement selon une logique complexe en plusieurs étapes qui peut s'exécuter pendant de longues périodes. Invoqué de manière asynchrone, il n'est donc pas limité par la limite de durée d'exécution du mappage de la source d'événements.

Mise en œuvre

La fonction intermédiaire reçoit l'intégralité de l'événement à partir du mappage de la source d'événements et invoque la fonction durable de manière asynchrone. Utilisez le paramètre du nom d'exécution pour vous assurer que l'exécution idempotente démarre, empêchant ainsi le traitement dupliqué si le mappage de la source d'événements tente à nouveau :

TypeScript

```
import { LambdaClient, InvokeCommand } from '@aws-sdk/client-lambda';
import { SQSEvent } from 'aws-lambda';
import { createHash } from 'crypto';

const lambda = new LambdaClient({});

export const handler = async (event: SQSEvent) => {
  // Invoke durable function asynchronously with execution name
  await lambda.send(new InvokeCommand({
    FunctionName: 'arn:aws:lambda:us-east-1:123456789012:function:my-durable-
function:1',
    InvocationType: 'Event',
    Payload: JSON.stringify({
      executionName: event.Name,
      event: event
    })
  }));

  return { statusCode: 200 };
};
```

Python

```
import boto3
import json
import hashlib

lambda_client = boto3.client('lambda')

def handler(event, context):
    # Invoke durable function asynchronously with execution name
```

```
    lambda_client.invoke(
        FunctionName='arn:aws:lambda:us-east-1:123456789012:function:my-durable-
function:1',
        InvocationType='Event',
        Payload=json.dumps({
            'executionName': execution_name,
            'event': event["name"]
        })
    )

    return {'statusCode': 200}
```

Pour garantir l'idempuissance de la fonction intermédiaire elle-même, utilisez Powertools for AWS Lambda afin d'éviter les appels dupliqués de la fonction durable si le mappage de la source d'événements tente à nouveau la fonction intermédiaire.

La fonction durable reçoit la charge utile avec le nom de l'exécution et traite tous les enregistrements selon une logique de longue durée :

TypeScript

```
import { withDurableExecution, DurableContext } from '@aws/durable-execution-sdk-
js';

export const handler = withDurableExecution(
  async (payload: any, context: DurableContext) => {
    const sqsEvent = payload.event;

    // Process each record with complex, multi-step logic
    const results = await context.map(
      sqsEvent.Records,
      async (ctx, record) => {
        const validated = await ctx.step('validate', async () => {
          return validateOrder(JSON.parse(record.body));
        });

        // Wait for external approval (could take hours or days)
        const approval = await ctx.waitForCallback(
          'approval',
          async (callbackId) => {
```

```
            await requestApproval(callbackId, validated);
          },
          { timeout: { hours: 48 } }
        );

        // Complete processing
        return await ctx.step('complete', async () => {
          return completeOrder(validated, approval);
        });
      }
    );

    return { statusCode: 200, processed: results.getResults().length };
  }
);
```

Python

```
from aws_durable_execution_sdk_python import durable_execution, DurableContext
from aws_durable_execution_sdk_python.config import Duration, WaitForCallbackConfig
from collections.abc import Sequence
import json

def validate_order(order_data: dict) -> dict:
    """Validate order data - always passes."""
    return order_data

def request_approval(callback_id: str, validated_order: dict) -> None:
    """Request approval for the order - always passes."""
    pass

def complete_order(validated_order: dict, approval_result: str) -> dict:
    """Complete the order processing - always passes."""
    return validated_order

@durable_execution
def lambda_handler(payload, context: DurableContext):
    sqs_event = payload['event']

    def process_record(
        ctx: DurableContext,
```

```
        record: dict,
        index: int,
        items: Sequence[dict]
    ) -> dict:
        validated = ctx.step(
            lambda _: validate_order(json.loads(record['body'])),
            name=f'validate-{index}'
        )

        approval = ctx.wait_for_callback(
            submitter=lambda callback_id, wait_ctx: request_approval(callback_id,
validated),
            name=f'approval-{index}',
            config=WaitForCallbackConfig(timeout=Duration.from_seconds(172800))
        )

        return ctx.step(
            lambda _: complete_order(validated, approval),
            name=f'complete-{index}'
        )

    results = context.map(
        inputs=sqs_event['Records'],
        func=process_record,
        name='process-records'
    )

    return {
        'statusCode': 200,
        'started': results.started_count,
        'completed': results.success_count,
        'failed': results.failure_count,
        'total': results.total_count
    }
```

Considérations clés

Ce modèle supprime la limite de durée d'exécution du mappage des sources d'événements en découplant le mappage des sources d'événements de l'exécution durable. La fonction intermédiaire revient immédiatement après le début de l'exécution durable, ce qui permet au mappage de la

source d'événements de poursuivre le traitement. La fonction durable fonctionne ensuite de manière indépendante aussi longtemps que nécessaire.

La fonction intermédiaire réussit lorsqu'elle invoque la fonction durable, et non lorsque l'exécution durable est terminée. Si l'exécution durable échoue ultérieurement, le mappage de la source d'événements ne réessaiera pas car le lot a déjà été traité avec succès. Implémentez la gestion des erreurs dans la fonction durable et configurez des files d'attente contenant des lettres mortes en cas d'échec d'exécution.

Utilisez le paramètre du nom d'exécution pour vous assurer que l'exécution idempotente démarre. Si le mappage de la source d'événements tente à nouveau la fonction intermédiaire, la fonction durable ne démarrera pas une double exécution car le nom de l'exécution existe déjà.

Sources d'événements prises en charge

Les fonctions durables prennent en charge toutes les sources d'événements Lambda qui utilisent des mappages de sources d'événements :

- Files d'attente Amazon SQS (standard et FIFO)
- Flux Kinesis
- DynamoDB Streams
- Amazon Managed Streaming for Apache Kafka (Amazon MSK)
- Self-managed Apache Kafka
- Amazon MQ (ActiveMQ et RabbitMQ)
- Flux de modifications d'Amazon DocumentDB

Tous les types de sources d'événements sont soumis à la limite d'exécution durable décrite précédemment (15 minutes par défaut) lors de l'appel de fonctions durables. Sur les instances gérées Lambda, la limite passe à 90 minutes pour ces sources d'événements, à l'exception d'Amazon MQ et d'Amazon DocumentDB, qui restent limitées à 15 minutes.

Réessais pour les fonctions durables de Lambda

Les fonctions durables offrent des fonctionnalités de relance automatique qui permettent à vos applications de résister aux défaillances transitoires. Le SDK gère les nouvelles tentatives à deux niveaux : les tentatives par étapes en cas d'échec de la logique métier et les tentatives du backend en cas de défaillance de l'infrastructure.

Étape 2 : Réessaie

Lorsqu'une exception non détectée se produit au cours d'une étape, le SDK réessaie automatiquement l'étape en fonction de la stratégie de nouvelle tentative configurée. Les tentatives d'étape sont des opérations ponctuelles qui permettent au SDK de suspendre l'exécution et de la reprendre ultérieurement sans perdre la progression.

Étape 1 : comportement de nouvelle tentative

Le tableau suivant décrit comment le SDK gère les exceptions par étapes :

Scénario	Que se passe-t-il	Impact du mesurage
Exception en cours avec les tentatives de nouvelle tentative restantes	Le SDK crée un point de contrôle pour la nouvelle tentative et suspend la fonction. Lors de l'appel suivant, l'étape réessaie avec le délai d'attente configuré.	1 opération+erreur sur la taille de la charge utile
Exception en cours, aucune nouvelle tentative n'étant restée	L'étape échoue et génère une exception. Si le code de votre gestionnaire ne détecte pas cette exception, l'exécution complète échoue.	1 opération+erreur sur la taille de la charge utile

Lorsqu'une étape doit être réessayée, le SDK vérifie l'état de nouvelle tentative et quitte l'appel Lambda si aucune autre tâche n'est en cours d'exécution. Cela permet au SDK d'implémenter des délais de temporisation sans consommer de ressources informatiques. La fonction reprend automatiquement après la période d'attente.

Configuration des stratégies de nouvelle tentative d'étape

Configurez des stratégies de nouvelle tentative pour contrôler la manière dont les étapes gèrent les échecs. Vous pouvez spécifier le nombre maximum de tentatives, les intervalles d'attente et les conditions de réessai. Pour une référence complète sur les aides à la stratégie de relance, les préréglages et les stratégies personnalisées, voir Rétentatives dans la documentation du SDK d'exécution durable.

Exceptions en dehors des étapes

Lorsqu'une exception non détectée se produit dans le code de votre gestionnaire mais en dehors de toute étape, le SDK marque l'exécution comme ayant échoué. Cela garantit que les erreurs dans la logique de votre application sont correctement capturées et signalées.

Scénario	Que se passe-t-il	Impact du mesurage
Exception dans le code du gestionnaire en dehors de toute étape	Le SDK marque l'exécuti on comme ayant échoué et renvoie l'erreur. L'exception n'est pas automatiquement réessayée.	Erreur concernant la taille de la charge utile

Pour activer la nouvelle tentative automatique pour le code sujet aux erreurs, associez-le à une étape avec une stratégie de nouvelle tentative. Les étapes fournissent une nouvelle tentative automatique avec une interruption configurable, tandis que le code en dehors des étapes échoue immédiatement.

Nouvelles tentatives d'invocation

Les tentatives au niveau de l'invocation sont gérées différemment selon la manière dont la fonction durable Lambda est tentée d'être invoquée. Le tableau suivant décrit comment les différents types d'invocation peuvent influencer le niveau des nouvelles tentatives d'appel.

Types d’invocation	Que se passe-t-il
Invocation synchrone	Lambda ne réessaie pas automatiquement l'invocation en cas d'erreur lors de l'exécution d'une fonction durable. Les nouvelles tentatives en cas d'échec d'invocation dépendent de la source de l'invocation synchrone. Par exemple, en utilisant le AWS SDK, InternalFailure et ThrottlingException sont réessayés automatiquement par défaut.
invocation asynchrone	Si l'exécution d'une fonction durable échoue (par exemple, si elle passe au statut FAILED, STOPPED ou TIMED_OUT), Lambda ne réessaie pas l'exécution.

Types d’invocation	Que se passe-t-il
	Cela est différent des fonctions sans exécution durable, où Lambda réessaie la fonction en cas d'échec d'appel asynchrone. Le `MaximumRetryAttempts` paramètre pour les appels asynchrones ne s'applique pas aux exécutions durables. Si vous configurez une file d'attente de lettres mortes (DLQ) pour la fonction, Lambda envoie l'événement déclencheur à la DLQ.
ESM (mappage des sources d'événements)	Lambda réessaie par défaut l'intégralité du lot jusqu'à ce qu'il réussisse. Pour les sources de flux (DynamoDB et Kinesis), vous pouvez configurer le nombre maximal de tentatives que Lambda effectue lorsque votre fonction renvoie une erreur. Voir le traitement par lots des mappages de sources d'événements. Pour Amazon SQS ESM, vous pouvez configurer le nombre maximum de tentatives via un DLQ sur la file d'attente Amazon SQS d'origine. Voir configurer Amazon SQS ESM. La meilleure pratique consiste à envisager une DLQ au niveau de la fonction et Lambda envoie l'événement déclencheur défaillant à la DLQ. Voir fonction DLQ.

Types d’invocation	Que se passe-t-il
Déclencheur direct	Cela dépend du « déclencheur ». Par exemple, Lambda traite les fonctions déclenchées par les notifications d'événements Amazon S3 de manière asynchron e. Consultez Traiter les notifications d'événements Amazon SQS avec Lambda. Lambda traite les fonctions déclenchées par les notifications d'événements Amazon SNS de manière asynchrone. Consultez Invoquer des fonctions Lambda avec les notifications Amazon SNS. Le comportement des nouvelles tentatives d'appel asynchrone est indiqué ci-dessus dans l'entrée du tableau « Invocation asynchrone ». Si Amazon SNS ne peut pas atteindre Lambda ou si le message est rejeté, Amazon SNS effectue de nouvelles tentatives à intervall es croissants pendant plusieurs heures. Pour plus de détails, consultes Fiabilité dans le FAQ sur Amazon SNS. API Gateway invoque Lambda de manière synchrone et renvoie la véritable réponse d'erreur au demandeur. Voir les nouvelles tentatives d'invocation. Le comportem ent des nouvelles tentatives d'invocation synchrone est indiqué ci-dessus dans l'entrée du tableau « Invocation synchrone ». Consultez chaque déclencheur direct pour plus de détails.

Rétentatives du backend

Les nouvelles tentatives du backend ont lieu lorsque Lambda rencontre des défaillances d'infrastructure, des erreurs d'exécution ou lorsque le SDK ne peut pas communiquer avec le service d'exécution durable. Lambda réessaie automatiquement ces défaillances pour aider vos fonctions durables à se remettre de problèmes d'infrastructure transitoires.

Scénarios de nouvelle tentative du backend

Lambda réessaie automatiquement votre fonction lorsqu'elle rencontre les scénarios suivants :

- Erreurs de service internes : lorsque Lambda ou le service d'exécution durable renvoie une erreur 5xx, indiquant un problème de service temporaire.
- Limitation : lorsque votre fonction est limitée en raison de limites de simultanéité ou de quotas de service.
- Délais d'expiration : lorsque le SDK ne parvient pas à atteindre le service d'exécution durable dans le délai imparti.
- Échec de l'initialisation du sandbox : lorsque Lambda ne parvient pas à initialiser l'environnement d'exécution.
- Erreurs d'exécution : lorsque le moteur d'exécution Lambda rencontre des erreurs extérieures au code de votre fonction, telles que des erreurs liées à un manque de mémoire ou des pannes de processus.
- Erreurs de jeton de point de contrôle non valides : lorsque le jeton de point de contrôle n'est plus valide, généralement en raison de changements d'état côté service.

Le tableau suivant décrit comment le SDK gère ces scénarios :

Scénario	Que se passe-t-il	Impact du mesurage
Erreur d'exécution en dehors du gestionnaire durable (OOM, délai d'attente, crash)	Lambda réessaie automatiquement l'appel. Le SDK se rejoue depuis le dernier point de contrôle, en sautant les étapes terminées.	Taille de la charge utile d'erreur + 1 opération par nouvelle tentative
Erreur de service (5xx) ou délai d'expiration lors de l'appel `CheckpointDurableExecution` à/APIs `GetDurableExecutionState`	Lambda réessaie automatiquement l'appel. Le SDK se rejoue depuis le dernier point de contrôle.	Taille de la charge utile d'erreur + 1 opération par nouvelle tentative
Throttling (429) ou jeton de point de contrôle non valide lors de l'appel à/APIs `CheckpointDurableExecution`	Lambda réessaie automatiquement l'invocation avec un retard exponentiel. Le SDK se rejoue depuis le dernier point de contrôle.	Taille de la charge utile d'erreur + 1 opération par nouvelle tentative

Scénario	Que se passe-t-il	Impact du mesurage
`GetDurableExecutionState`		
Erreur client (4xx, sauf 429 et jeton non valide) lorsque`CheckpointDurableExecution` /`GetDurableExecutionState` APIs	Le SDK marque l'exécution comme ayant échoué. Aucune nouvelle tentative automatique ne se produit car l'erreur indique un problème permanent.	Erreur concernant la taille de la charge utile

Les nouvelles tentatives du backend utilisent un retard exponentiel et se poursuivent jusqu'à ce que la fonction réussisse ou que le délai d'exécution soit atteint. Pendant la rediffusion, le SDK ignore les points de contrôle terminés et poursuit l'exécution depuis la dernière opération réussie, garantissant ainsi que votre fonction ne réexécute pas le travail terminé.

Réessayez les meilleures pratiques

Suivez les meilleures pratiques suivantes lors de la configuration des stratégies de nouvelle tentative :

- Configurez des stratégies de relance explicites : ne vous fiez pas au comportement de nouvelle tentative par défaut en production. Configurez des stratégies de nouvelles tentatives explicites avec un nombre maximum de tentatives et des intervalles d'attente adaptés à votre cas d'utilisation.
- Utiliser des tentatives conditionnelles : implémentez une `shouldRetry` logique permettant de réessayer uniquement les erreurs transitoires (limites de débit, délais d'attente) et d'échouer rapidement en cas d'erreur permanente (échec de validation, introuvable).
- Définissez le nombre maximum de tentatives approprié : équilibre entre résilience et temps d'exécution. Un trop grand nombre de tentatives peut retarder la détection des échecs, tandis qu'un nombre insuffisant peut entraîner des échecs inutiles.
- Utilisez le ralentissement exponentiel : le ralentissement exponentiel réduit la charge sur les services en aval et augmente les chances de reprise après des défaillances transitoires.
- Enveloppez le code sujet aux erreurs par étapes : le code en dehors des étapes ne peut pas être réessayé automatiquement. Intégrez les appels d'API externes, les requêtes de base de données

et les autres opérations susceptibles d'entraîner des erreurs par étapes grâce à des stratégies de nouvelle tentative.

- Surveillez les statistiques relatives aux nouvelles tentatives : suivez les opérations de nouvelle tentative par étapes et les échecs d'exécution sur Amazon CloudWatch afin d'identifier les modèles et d'optimiser les stratégies de nouvelles tentatives.

Idempotence

Les fonctions durables fournissent une idempotence intégrée pour les démarrages d'exécution par le biais de noms d'exécution. Lorsque vous fournissez un nom d'exécution, Lambda l'utilise pour empêcher les exécutions dupliquées et permettre de nouvelles tentatives d'invocation en toute sécurité. Les étapes ont une sémantique d'exécution au moins une fois par défaut. Pendant la rediffusion, le SDK renvoie des résultats vérifiés sans réexécuter les étapes terminées, mais votre logique métier doit être idempotente pour gérer les nouvelles tentatives potentielles avant la fin.

> **Note**
>
> Les mappages de sources d'événements Lambda (ESM) ne prennent pas en charge l'idempotence au lancement. Par conséquent, chaque invocation (y compris les nouvelles tentatives) lance une nouvelle exécution durable. Pour garantir une exécution idempotente avec des mappages de sources d'événements, implémentez la logique d'idempotence dans le code de votre fonction, comme avec Powertools for, AWS Lambda ou utilisez une fonction Lambda classique comme proxy (répartiteur) pour invoquer une fonction durable avec une clé d'idempotence (paramètre du nom d'exécution).

Noms d'exécution

Vous pouvez fournir un nom d'exécution lorsque vous invoquez une fonction durable. Le nom de l'exécution agit comme une clé d'idempotence, vous permettant de réessayer les demandes d'invocation en toute sécurité sans créer d'exécutions dupliquées. Si vous ne fournissez pas de nom, Lambda génère automatiquement un identifiant d'exécution unique.

Les noms d'exécution doivent être uniques au sein de votre compte et de votre région. Lorsque vous appelez une fonction dont le nom d'exécution existe déjà, le comportement de Lambda dépend de l'état de l'exécution existante et de la correspondance de la charge utile.

Comportement d'idempotence

Le tableau suivant décrit la façon dont Lambda gère les demandes d'appel selon que vous fournissez un nom d'exécution, l'état d'exécution existant et si la charge utile correspond :

Scénario	Nom fourni ?	État d'exécution existant	Charge utile identique ?	Comportement
1	Non	N/A	N/A	Nouvelle exécution démarrée : Lambda génère un identifiant d'exécution unique et démarre une nouvelle exécution
2	Oui	N'a jamais existé ou la conservation a expiré	N/A	Nouvelle exécution démarrée : Lambda démarre une nouvelle exécution avec le nom fourni
3	Oui	En cours d'exécution	Oui	Démarrage idempotent : Lambda renvoie les informations d'exécution existantes sans créer de doublon. Pour les appels synchrones, cela agit comme un reattachement à l'exécution en cours
4	Oui	En cours d'exécution	Non	Erreur : Lambda renvoie une `DurableExecutionAlreadyStartedException`

Scénario	Nom fourni ?	État d'exécution existant	Charge utile identique ?	Comportement
				erreur car une exécution portant ce nom est déjà en cours d'exécution avec une charge utile différente
5	Oui	Fermé (succès, échec, arrêt ou expiration du délai)	Oui	Démarrage idempotent : Lambda renvoie les informations d'exécution existantes sans démarrer une nouvelle exécution. Le résultat de l'exécution fermée est renvoyé
6	Oui	Fermé (succès, échec, arrêt ou expiration du délai)	Non	Erreur : Lambda renvoie une `DurableExecutionAlreadyStartedException` erreur car une exécution portant ce nom s'est déjà terminée avec une charge utile différente

Remarque

Les scénarios 3 et 5 présentent un comportement idempotent dans lequel Lambda gère en toute sécurité les demandes d'invocation dupliquées en renvoyant les informations d'exécution existantes au lieu de créer des doublons.

Étape 1 : empotence

Les étapes ont une sémantique d'exécution au moins une fois par défaut. Lorsque votre fonction est rejouée après une attente, un rappel ou un échec, le SDK vérifie chaque étape par rapport au journal des points de contrôle. Pour les étapes déjà terminées, le SDK renvoie le résultat du point de contrôle sans réexécuter la logique des étapes. Toutefois, si une étape échoue ou si la fonction est interrompue avant la fin de l'étape, celle-ci peut être exécutée plusieurs fois.

La logique métier qui sous-tend vos étapes doit être idempotente pour gérer d'éventuelles nouvelles tentatives. Utilisez des clés d'idempotence pour vous assurer que les opérations telles que les paiements ou les écritures de bases de données ne s'exécutent qu'une seule fois, même si l'étape est relancée. Consultez la section Idempotence et nouvelles tentatives dans le Guide du développeur du SDK AWS Durable Execution pour plus de détails sur la façon de coder pour l'idempotence.

Tester les fonctions durables de Lambda

Utilisez les SDK de test d'exécution durable pour exécuter et inspecter les exécutions en local et dans le cloud. Pour la création de tests, d'assertions, le cloud runner, l'intégration de la CLI SAM et des exemples complets, consultez la section Testing in the AWS Durable Execution SDK Developer Guide.

Autorisations IAM pour les tests dans le cloud

Lorsque vous utilisez le cloud runner ou `sam remote invoke` que vous testez une fonction durable déployée, le principal appelant doit être autorisé à invoquer la fonction et à lire son historique d'exécution. Attachez les autorisations suivantes à votre interlocuteur test :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "lambda:InvokeFunction",
                "lambda:GetDurableExecution",
                "lambda:GetDurableExecutionHistory"
            ],
            "Resource": [
```

```
                "arn:aws:lambda:region:account-id:function:function-name",
                "arn:aws:lambda:region:account-id:function:function-name:*"
            ]
        }
    ]
}
```

Remplacez *regionaccount-id*, et *function-name* par vos valeurs.

Défaillances de débogage

Lorsque les tests échouent, inspectez le résultat de l'exécution pour comprendre ce qui s'est mal passé. Vérifiez l'état d'exécution pour voir si la fonction a réussi, a échoué ou a expiré. Lisez les messages d'erreur pour comprendre la cause de l'échec.

Inspectez les résultats de chaque opération pour trouver les domaines dans lesquels le comportement ne correspondait pas aux attentes. Vérifiez les résultats des étapes pour voir quelles valeurs ont été produites. Vérifiez l'ordre des opérations pour confirmer que les opérations sont exécutées dans l'ordre attendu. Comptez les opérations pour vous assurer que le bon nombre d'étapes, d'attentes et de rappels a été créé.

Les problèmes courants incluent le code non déterministe qui produit des résultats différents lors de la réexécution, l'état partagé par le biais de variables globales qui s'interrompent pendant la rediffusion et les opérations manquantes en raison d'erreurs de logique conditionnelle. Utilisez les débogueurs et la journalisation standard pour parcourir le code de fonction et suivre le flux d'exécution.

Pour les tests dans le cloud, consultez l'historique des exécutions dans CloudWatch les journaux pour consulter les journaux d'opérations détaillés. Utilisez le suivi pour suivre le flux d'exécution entre les services et identifier les goulots d'étranglement.

Surveillance des fonctions durables

Vous pouvez surveiller vos fonctions durables à l'aide de CloudWatch des indicateurs, CloudWatch Journaux et traçage. Étant donné que les fonctions durables peuvent s'exécuter pendant de longues périodes et couvrir plusieurs appels de fonctions, leur surveillance nécessite de comprendre leurs modèles d'exécution uniques, notamment les points de contrôle, les transitions d'état et le comportement de relecture.

> **Note**
>
> Pour plus d'informations sur les quotas applicables aux fonctions durables, voir Quotas de fonctions durables.

CloudWatch indicateurs

Lambda publie automatiquement des métriques sur CloudWatch sans frais supplémentaires. Les fonctions durables fournissent des mesures supplémentaires au-delà des mesures Lambda standard pour vous aider à surveiller les flux de travail de longue durée, la gestion des états et l'utilisation des ressources.

Métriques d'exécution durables

Lambda émet les métriques suivantes pour des exécutions durables :

Métrique	Description
`ApproximateRunningDurableExecutions`	Nombre d'exécutions durables en état de marche
`ApproximateRunningDurableExecutionsUtilization`	Pourcentage du quota maximal d'exécutions durables en cours d'exécution de votre compte actuellement utilisé
`DurableExecutionDuration`	Temps d'horloge murale écoulé en millisecondes pendant lequel une exécution durable est restée à l'état RUNNING
`DurableExecutionStarted`	Nombre d'exécutions durables qui ont commencé
`DurableExecutionStopped`	Nombre d'exécutions durables qui ont cessé d'utiliser le StopDurableExecution API
`DurableExecutionSucceeded`	Nombre d'exécutions durables qui ont été menées à bien
`DurableExecutionFailed`	Nombre d'exécutions durables qui se sont terminées par un échec

Métrique	Description
`DurableExecutionTimedOut`	Nombre d'exécutions durables qui ont dépassé le délai d'exécution configuré
`DurableExecutionOperations`	Nombre cumulé d'opérations effectuées dans le cadre d'une exécution durable
`DurableExecutionStorageWrittenBytes`	Quantité cumulée de données en octets conservée par une exécution durable

CloudWatch indicateurs

Lambda émet des mesures d'appel, de performance et de simultanéité standard pour des fonctions durables. Dans la mesure où une exécution durable peut couvrir plusieurs appels de fonctions au fur et à mesure qu'elle passe par des points de contrôle et des rediffusions, ces métriques se comportent différemment de celles des fonctions standard :

- Invocations : Compte chaque appel de fonction, y compris les rediffusions. Une seule exécution durable peut générer plusieurs points de données d'invocation.
- Durée : Mesure l'invocation de chaque fonction séparément. Utiliser `DurableExecutionDuration` pour le temps total nécessaire à une seule exécution durable.
- Erreurs : Suit les échecs d'invocation des fonctions. Utiliser `DurableExecutionFailed` pour les échecs au niveau de l'exécution.

Pour une liste complète des métriques Lambda standard, voir Types de métriques pour les fonctions Lambda.

Création CloudWatch alarmes

Créez CloudWatch des alarmes pour vous avertir lorsque les métriques dépassent les seuils. Les alarmes les plus courantes sont les suivantes :

- `ApproximateRunningDurableExecutionsUtilization` dépasse 80 % de votre quota
- `DurableExecutionFailed` augmente au-dessus d'un seuil
- `DurableExecutionTimedOut` indique que les exécutions arrivent à expiration
- `DurableExecutionStorageWrittenBytes` approche les limites de stockage

Pour plus d'informations, voir En utilisant CloudWatch alarmes.

EventBridge événements

Lambda publie des événements de changement d'état d'exécution durables pour EventBridge. Vous pouvez utiliser ces événements pour déclencher des flux de travail, envoyer des notifications ou suivre les modifications du cycle de vie d'exécution de vos fonctions durables.

Événements durables de changement de statut d'exécution

Lambda émet un événement pour EventBridge chaque fois qu'une exécution durable change de statut. Ces événements présentent les caractéristiques suivantes :

- Source : `aws.lambda`
- Type de détail : `Durable Execution Status Change`

Les événements de changement de statut sont publiés pour les états d'exécution suivants :

- `RUNNING` - L'exécution a commencé
- `SUCCEEDED` - Exécution terminée avec succès
- `STOPPED` - L'exécution s'est arrêtée à l'aide du StopDurableExecution API
- `FAILED` - L'exécution a échoué avec une erreur
- `TIMED_OUT` - L'exécution a dépassé le délai d'attente configuré

L'exemple suivant illustre un événement de changement durable du statut d'exécution :

```
{
  "version": "0",
  "id": "d019b03c-a8a3-9d58-85de-241e96206538",
  "detail-type": "Durable Execution Status Change",
  "source": "aws.lambda",
  "account": "123456789012",
  "time": "2025-11-20T13:08:22Z",
  "region": "us-east-1",
  "resources": [],
  "detail": {
    "durableExecutionArn": "arn:aws:lambda:us-east-1:123456789012:function:my-function:
$LATEST/durable-execution/090c4189-b18b-4296-9d0c-cfd01dc3a122/9f7d84c9-ea3d-3ffc-
b3e5-5ec51c34ffc9",
```

```
    "durableExecutionName": "order-123",
    "functionArn": "arn:aws:lambda:us-east-1:123456789012:function:my-function:2",
    "status": "RUNNING",
    "startTimestamp": "2025-11-20T13:08:22.345Z"
  }
}
```

Pour les états terminaux (`SUCCEEDED`, `STOPPED`, `FAILED`, `TIMED_OUT`), l'événement comprend un `endTimestamp` champ indiquant la date de fin de l'exécution.

Création EventBridge règles

Créez EventBridge règles pour acheminer les événements de modification durable de l'état d'exécution vers des cibles telles qu'Amazon Simple Notification Service, Amazon Simple Queue Service ou d'autres fonctions Lambda.

L'exemple suivant crée une règle qui correspond à toutes les modifications durables du statut d'exécution :

```
{
  "source": ["aws.lambda"],
  "detail-type": ["Durable Execution Status Change"]
}
```

L'exemple suivant crée une règle qui ne correspond qu'aux exécutions ayant échoué :

```
{
  "source": ["aws.lambda"],
  "detail-type": ["Durable Execution Status Change"],
  "detail": {
    "status": ["FAILED"]
  }
}
```

L'exemple suivant crée une règle qui correspond aux changements de statut pour une fonction spécifique :

```
{
  "source": ["aws.lambda"],
  "detail-type": ["Durable Execution Status Change"],
  "detail": {
    "functionArn": [{
      "prefix": "arn:aws:lambda:us-east-1:123456789012:function:my-function"
    }]
  }
}
```

Pour plus d'informations sur la création EventBridge règles, voir Amazon EventBridge tutoriels dans le EventBridge Guide de l'utilisateur

Utiliser les files d'attente aux lettres mortes avec EventBridge événements

EventBridge les événements de changement d'état fournissent une notification en temps réel lorsqu'une exécution durable passe à l'état FAILED, STOPPED ou TIMED_OUT, mais ils n'incluent pas la charge utile de l'événement d'origine qui a déclenché l'exécution. Pour capturer l'événement déclencheur en vue d'une analyse ou d'un retraitement ultérieur, configurez une file d'attente de lettres mortes (DLQ) sur votre fonction durable.

Lorsqu'une exécution durable échoue après un appel asynchrone, Lambda envoie l'événement déclencheur d'origine au DLQ configuré. Utiliser EventBridge événements et DLQ combinés pour une stratégie complète de gestion des pannes :

- EventBridge événements — Déclenchez des alertes immédiates, mettez à jour les tableaux de bord ou lancez des flux de travail de correction lorsque les exécutions échouent.
- Dead-letter files d'attente — Préservez la charge utile de l'événement d'origine afin de pouvoir inspecter la cause de la panne, déboguer le problème et éventuellement retraiter l'événement après avoir résolu le problème sous-jacent.

Pour plus d'informations sur la configuration d'un DLQ sur votre fonction, voir Dead-letter files d'attente.

AWS X-Ray suivi

Vous pouvez activer X-Ray traçage de vos fonctions durables. Lambda passe le X-Ray trace l'en-tête vers l'exécution durable, vous permettant de suivre les demandes tout au long de votre flux de travail.

Pour activer X-Ray; traçage à l'aide de la console Lambda, choisissez votre fonction, puis choisissez Outils de configuration, de surveillance et d'exploitation, puis activez le suivi actif sous X-Ray.

Pour activer X-Ray traçage à l'aide du AWS CLI:

```
aws lambda update-function-configuration \
    --function-name my-durable-function \
    --tracing-config Mode=Active
```

Pour activer AWS X-Ray traçage à l'aide AWS SAM:

```
Resources:
  MyDurableFunction:
    Type: AWS::Serverless::Function
    Properties:
      Tracing: Active
      DurableConfig:
        ExecutionTimeout: 3600
```

Pour plus d'informations sur X-Ray, consultez le AWS X-Ray Guide du développeur.

Bonnes pratiques pour les fonctions durables de Lambda

Les fonctions durables utilisent un modèle d'exécution basé sur le replay qui nécessite des pratiques de programmation différentes de celles des fonctions Lambda traditionnelles. Consultez les meilleures pratiques du Guide du développeur du SDK d'exécution AWS durable pour obtenir des conseils sur la façon d'écrire et de tester du code de flux de travail durable.

Les recommandations suivantes constituent les meilleures pratiques pour le déploiement, l'appel et la surveillance des fonctions durables Lambda.

Versions et alias des fonctions

Invoquez des fonctions avec des numéros de version ou des alias pour associer les exécutions à des versions de code spécifiques. Assurez-vous que les nouvelles versions du code peuvent gérer l'état des anciennes versions. Ne renommez pas les étapes et ne modifiez pas leur comportement

de manière à interrompre la rediffusion. Si vous renommez une étape ou modifiez son comportement alors que des exécutions sont en cours, ces exécutions peuvent échouer ou produire des résultats incorrects. Cela se produit parce que le moteur d'exécution ne peut plus faire correspondre l'état enregistré à la définition d'étape attendue.

Contrôle

Activez la journalisation structurée avec les identifiants d'exécution et les noms des étapes. Configurez CloudWatch des alarmes pour les taux d'erreur et la durée d'exécution. Utilisez le traçage pour identifier les goulots d'étranglement. Pour obtenir des instructions détaillées, consultez la section Surveillance et débogage.

Gestion des erreurs

Outre la configuration de stratégies de nouvelle tentative pour les échecs transitoires, configurez une file d'attente de lettres mortes (DLQ) sur votre fonction durable afin de capturer les événements liés à des échecs permanents d'exécutions. Lorsqu'une exécution durable atteint un état terminal (FAILED, STOPPED ou TIMED_OUT) après un appel asynchrone, Lambda envoie l'événement déclencheur d'origine au DLQ. Ainsi, vous pouvez inspecter, déboguer et éventuellement retraiter les événements ayant échoué sans les perdre.

Pour configurer un DLQ, définissez la `DeadLetterConfig` propriété de votre fonction sur une file d'attente Amazon SQS ou un ARN de rubrique Amazon SNS. Pour plus d'informations, consultez la section Dead-letter files d'attente.

Suivez les meilleures pratiques suivantes pour gérer les erreurs avec des fonctions durables :

- Configurer un DLQ pour les invocations asynchrones : attachez toujours une file d'attente de lettres mortes lorsque vous invoquez des fonctions durables de manière asynchrone. Contrairement aux appels asynchrones de fonctions sans exécution durable, Lambda ne réessaie pas automatiquement les exécutions durables en cas d'échec. Une DLQ correctement configurée capture les événements qui ont entraîné l'échec définitif des exécutions. Assurez-vous que le DLQ dispose des autorisations appropriées et d'une capacité suffisante pour recevoir des messages.
- Utilisez des stratégies de nouvelle tentative par étapes : configurez des stratégies de nouvelle tentative explicites avec un délai approprié pour les échecs transitoires. Pour obtenir des conseils sur la configuration des nouvelles tentatives, voir Rétentatives pour des fonctions durables.
- Combinez les DLQ avec EventBridge les notifications : utilisez des EventBridge règles pour signaler les changements de statut FAILED, STOPPED et TIMED_OUT pour une visibilité en

temps réel, et utilisez une DLQ pour conserver la charge utile de l'événement d'origine en vue d'une analyse ou d'un retraitement ultérieurs.

- Surveillez la profondeur de la DLQ : créez une CloudWatch alarme sur la `ApproximateNumberOfMessagesVisible` métrique pour que votre DLQ détecte les défaillances qui s'accumulent.

Ressources connexes

- AWS Guide du développeur du SDK d'exécution durable
- Surveillance des fonctions durables de Lambda
- Réessais pour les fonctions durables de Lambda
- Tester les fonctions durables de Lambda

Améliorer les performances de démarrage avec Lambda SnapStart

Lambda SnapStart peut fournir des performances de démarrage inférieures à une seconde, généralement sans modification du code de votre fonction d'événement. SnapStart facilite la création d'applications hautement réactives et évolutives sans provisionnement de ressources ni mise en œuvre d'optimisations complexes des performances.

Le principal facteur de latence au démarrage (souvent appelé temps de démarrage à froid) est le temps que Lambda passe à initialiser la fonction, ce qui inclut le chargement du code de la fonction, le démarrage de l'environnement d'exécution et l'initialisation du code de la fonction. Avec SnapStart, Lambda initialise votre fonction d'événement lorsque vous publiez une version de fonction. Lambda prend un instantané Firecracker MicroVM de l'état de la mémoire et du disque de l'environnement d'exécution initialisé, chiffre l'instantané et le met en cache de manière intelligente pour optimiser la latence de récupération.

Pour garantir la résilience, Lambda conserve plusieurs copies de chaque instantané. Lambda corrige automatiquement les instantanés et leurs copies avec les dernières mises à jour de sécurité et de l'environnement d'exécution. Lorsque vous appelez la version Event Function pour la première fois, et à mesure que les appels augmentent, Lambda reprend les nouveaux environnements d'exécution à partir de l'instantané mis en cache au lieu de les initialiser à partir de zéro, ce qui améliore la latence de démarrage.

> **Important**
>
> Si vos applications dépendent de l'unicité de l'état, vous devez évaluer votre code de fonction et vérifier qu'il est résilient aux opérations instantanées. Pour plus d'informations, consultez Gérer l'unicité avec Lambda SnapStart.

Si vous rencontrez des problèmes, consultezthe section called "Résolution des problèmes".

Rubriques

- Quand utiliser SnapStart
- Fonctions prises en charge et limitations
- Régions prises en charge
- Considérations de compatibilité
- SnapStart tarification
- Activation et gestion de Lambda SnapStart
- Gérer l'unicité avec Lambda SnapStart
- Implémenter le code avant ou après les instantanés de la fonction d'événement Lambda
- Surveillance pour Lambda SnapStart
- Modèle de sécurité pour Lambda SnapStart
- Maximisez les performances Lambda SnapStart
- Résolution des SnapStart erreurs liées aux fonctions d'événement Lambda

Quand utiliser SnapStart

Lambda SnapStart est conçu pour remédier à la variabilité de latence introduite par un code d'initialisation unique, tel que le chargement de dépendances de modules ou de frameworks. Ces opérations peuvent parfois prendre plusieurs secondes lors de l'invocation initiale. SnapStart À utiliser pour réduire cette latence de quelques secondes à une valeur inférieure à une seconde, dans des scénarios optimaux. SnapStart fonctionne mieux lorsqu'il est utilisé avec des invocations de fonctions à grande échelle. Les fonctions qui sont rarement invoquées peuvent ne pas bénéficier des mêmes améliorations de performance.

SnapStart est particulièrement utile pour deux principaux types d'applications :

- Latency-sensitive API et flux utilisateur : les fonctions faisant partie des points de terminaison critiques des API ou des flux destinés aux utilisateurs peuvent bénéficier de la réduction de SnapStart la latence et de l'amélioration des temps de réponse.
- Latency-sensitive flux de travail de traitement des Time-bound données : les flux de travail de traitement des données qui utilisent les fonctions d'événement Lambda peuvent améliorer le débit en réduisant le temps de latence d'initialisation des fonctions anormales.

La simultanéité provisionnée permet aux fonctions d'événement d'être initialisées et prêtes à répondre en quelques millisecondes à deux chiffres. Utilisez la simultanéité provisionnée si votre application a des exigences strictes en matière de latence de démarrage à froid auxquelles il est impossible de répondre de manière adéquate. SnapStart

Fonctions prises en charge et limitations

SnapStart prend en charge les environnements d'exécution gérés Lambda suivants et les images de base AWS Lambda correspondantes dans les formats de déploiement d'images ZIP et de conteneur :

- Java 11 et versions ultérieures
- Python 3.12 et versions ultérieures
- .NET 8 et versions ultérieures. Si vous utilisez le framework Lambda Annotations pour .NET, passez à la Amazon.Lambda.Annotationsversion 1.6.0 ou ultérieure pour garantir la compatibilité avec. SnapStart

Pour les images de conteneur créées à partir d'images de base AWS Lambda ou d'images de base personnalisées, consultez SnapStart Implémentation de crochets pour les images de conteneurs et validez votre code de fonction pour gérer les exigences d' SnapStart unicité.

Les autres environnements d'exécution gérés (tels que `nodejs24.x` et`ruby4.0`) ne OS-only runtimes sont pas pris en charge. SnapStart ne prend pas en charge la simultanéité provisionnée, Amazon Elastic File System (Amazon EFS), Amazon S3 Files ou le stockage éphémère supérieur à 512 Mo.

> **Note**
>
> Vous ne pouvez l'utiliser SnapStart que sur des versions de fonctions publiées et des alias pointant vers des versions. Vous ne pouvez pas l'utiliser SnapStart sur la version non publiée d'une fonction ($LATEST).

Régions prises en charge

Lambda SnapStart est disponible dans toutes les régions commerciales, à l'exception de l'Asie-Pacifique (Nouvelle Zélande) et de l'Asie-Pacifique (Taipei).

Considérations de compatibilité

Avec SnapStart, Lambda utilise un seul instantané comme état initial pour plusieurs environnements d'exécution. Si votre fonction utilise l'un des éléments suivants pendant la phase d'initialisation, vous devrez peut-être apporter quelques modifications avant de l'utiliser SnapStart :

Unicité

Si votre code d'initialisation génère un contenu unique qui est inclus dans l'instantané, ce contenu peut ne pas être unique lorsqu'il est réutilisé dans plusieurs environnements d'exécution. Pour conserver l'unicité lors de l'utilisation SnapStart, vous devez générer un contenu unique après l'initialisation. Cela inclut les identifiants uniques, les secrets uniques et l'entropie utilisée pour générer un pseudo aléatoire. Pour savoir comment restaurer l'unicité, consultez Gérer l'unicité avec Lambda SnapStart.

Connexions réseau

L'état des connexions que votre fonction d'événement établit pendant la phase d'initialisation n'est pas garanti lorsque Lambda reprend votre fonction à partir d'un instantané. Validez l'état de vos connexions réseau et rétablissez-les si nécessaire. Dans la plupart des cas, les connexions réseau établies par un AWS SDK reprennent automatiquement. Pour les autres connexions, consultez les bonnes pratiques.

Données temporaires

Certaines fonctions téléchargent ou initialisent des données éphémères, telles que des informations d'identification temporaires ou des horodatages mis en cache, pendant la phase d'initialisation. Actualisez les données éphémères dans le gestionnaire de fonctions avant de les utiliser, même lorsque vous ne les utilisez pas. SnapStart

SnapStart tarification

> **Note**
>
> Pour les environnements d'exécution gérés par Java, il n'y a aucun coût supplémentaire pour SnapStart. Vous êtes facturé en fonction du nombre de demandes pour vos fonctions, de la durée d'exécution de votre code et de la mémoire configurée pour votre fonction.

Le coût d'utilisation SnapStart inclut les éléments suivants :

- Mise en cache : pour chaque version de fonction que vous publiez avec cette SnapStart option activée, vous payez les frais de mise en cache et de maintenance de l'instantané. Le prix dépend de la quantité de mémoire que vous allouez à votre fonction. Vous êtes facturé pour un minimum de 3 heures.

  Vous continuez à être débité tant que votre fonction reste active. Utilisez l'action ListVersionsByFunctionAPI pour identifier les versions des fonctions, puis utilisez-la DeleteFunctionpour supprimer les versions inutilisées. Pour supprimer automatiquement les versions de fonction inutilisées, consultez le modèle Lambda Version Cleanup sur Serverless Land.
- Restauration : chaque fois qu'une instance de fonction est restaurée à partir d'un instantané, vous payez des frais de restauration. Le prix dépend de la quantité de mémoire que vous allouez à votre fonction.

Comme pour toutes les fonctions d'événement Lambda, des frais de durée s'appliquent au code exécuté dans le gestionnaire de fonctions. Pour les SnapStart fonctions, les frais de durée s'appliquent également au code d'initialisation déclaré en dehors du gestionnaire, au temps nécessaire au chargement de l'exécution et à tout code exécuté dans un hook d'exécution. La durée est calculée à partir du moment où votre code commence à s'exécuter jusqu'à son retour ou sa fin, arrondie à la milliseconde la plus proche. Lambda conserve des copies en cache de votre instantané pour des raisons de résilience et leur applique automatiquement les mises à jour logicielles, telles que les mises à niveau de l'environnement d'exécution et les correctifs de sécurité. Des frais s'appliquent chaque fois que Lambda réexécute votre code d'initialisation pour appliquer des mises à jour logicielles.

Pour plus d'informations sur le coût d'utilisation SnapStart, consultez la section AWS Lambda Tarification.

Activation et gestion de Lambda SnapStart

Pour l'utiliser SnapStart, activez-la SnapStart sur une fonction d'événement Lambda nouvelle ou existante. Ensuite, publiez et invoquez une version de la fonction.

Rubriques

- Activation SnapStart (console)
- Activation SnapStart (AWS CLI)
- Activation SnapStart (API)
- États des fonctions Lambda SnapStart et Event
- Mise à jour d’un instantané
- Utilisation SnapStart avec AWS Kits SDK
- Utilisation SnapStart avec CloudFormation, AWS SAM, et AWS CDK
- Suppression d’instantanés

Activation SnapStart (console)

SnapStart Pour activer une fonction événementielle

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez le nom d'une fonction événementielle.
3. Choisissez Configuration, puis General configuration (Configuration générale).
4. Dans le volet General configuration (Configuration générale), choisissez Edit (Modifier).
5. Sur la page Modifier les paramètres de base, pour SnapStart, choisissez Versions publiées.
6. Cliquez sur Enregistrer.
7. Publiez une version de la fonction. Lambda initialise votre code, crée un instantané de l’environnement d’exécution initialisé, puis met en cache l’instantané pour un accès à faible latence.
8. Invoquez la version de la fonction..

Activation SnapStart (AWS CLI)

SnapStart Pour activer une fonction événementielle existante

1. Mettez à jour la configuration de la fonction en exécutant la commande update-function-configuration avec l'option --snap-start.

```
aws lambda update-function-configuration \
  --function-name my-function \
  --snap-start ApplyOn=PublishedVersions
```

2. Publiez une version de la fonction avec la commande publish-version.

```
aws lambda publish-version \
  --function-name my-function
```

3. Vérifiez qu'elle SnapStart est activée pour la version de la fonction en exécutant la commande get-function-configuration et en spécifiant le numéro de version. L'exemple suivant spécifie la version 1.

```
aws lambda get-function-configuration \
  --function-name my-function:1
```

   Si la réponse indique que OptimizationStatusc'est le cas On et que State est activé`Active`, SnapStart il est activé et un instantané est disponible pour la version de fonction spécifiée.

```
"SnapStart": {
    "ApplyOn": "PublishedVersions",
    "OptimizationStatus": "On"
 },
 "State": "Active",
```

4. Invoquez la version de la fonction en exécutant la commande invoke et en spécifiant la version. L'exemple suivant invoque la version 1.

```
aws lambda invoke \
  --cli-binary-format raw-in-base64-out \
  --function-name my-function:1 \
  --payload '{ "name": "Bob" }' \
  response.json
```

L'cli-binary-formatoption est obligatoire si vous utilisez AWS CLI la version 2. Pour faire de ce paramètre le paramètre par défaut, exécutez `aws configure set cli-binary-format raw-in-base64-out`. Pour plus d'informations, consultez les options de ligne de commande globales AWS CLI prises en charge dans le Guide de l'utilisateur AWS Command Line Interface version 2.

À activer SnapStart lorsque vous créez une nouvelle fonction événementielle

1. Créez une fonction en exécutant la commande create-function avec l'option --snap-start. Pour --role, spécifiez le Amazon Resource Name (ARN) de votre rôle d'exécution.

   > **Note**
   >
   > Si vous utilisez une fonction SnapStart d'image de conteneur qui utilise des images de base autres que les images de AWS base de Lambda pour Java (version 11+), Python (version 3.12+) et .NET (version 8+), suivez les instructions SnapStart Implémentation de crochets pour les images de conteneurs pour rendre votre image compatible avec. SnapStart

   ```
   aws lambda create-function \
     --function-name my-function \
     --runtime "java25" \
     --zip-file fileb://my-function.zip \
     --handler my-function.handler \
     --role arn:aws:iam::111122223333:role/lambda-ex \
     --snap-start ApplyOn=PublishedVersions
   ```

2. Créez une version avec la commande publish-version.

   ```
   aws lambda publish-version \
     --function-name my-function
   ```

3. Vérifiez qu'elle SnapStart est activée pour la version de la fonction en exécutant la commande get-function-configuration et en spécifiant le numéro de version. L'exemple suivant spécifie la version 1.

   ```
   aws lambda get-function-configuration \
   ```

```
  --function-name my-function:1
```

Si la réponse indique que OptimizationStatusc'est le cas On et que State est activéActive, SnapStart il est activé et un instantané est disponible pour la version de fonction spécifiée.

```
"SnapStart": {
     "ApplyOn": "PublishedVersions",
     "OptimizationStatus": "On"
  },
  "State": "Active",
```

4. Invoquez la version de la fonction en exécutant la commande invoke et en spécifiant la version. L'exemple suivant invoque la version 1.

```
aws lambda invoke \
  --cli-binary-format raw-in-base64-out \
  --function-name my-function:1 \
  --payload '{ "name": "Bob" }' \
  response.json
```

L'cli-binary-formatoption est obligatoire si vous utilisez AWS CLI la version 2. Pour faire de ce paramètre le paramètre par défaut, exécutez `aws configure set cli-binary-format raw-in-base64-out`. Pour plus d'informations, consultez les options de ligne de commande globales AWS CLI prises en charge dans le Guide de l'utilisateur AWS Command Line Interface version 2.

Activation SnapStart (API)

Pour activer SnapStart

1. Effectuez l'une des actions suivantes :
   - Créez une nouvelle fonction d'événement SnapStart activée en utilisant l'action de l'CreateFunctionAPI avec le SnapStartparamètre.
   - SnapStart Activez une fonction événementielle existante en utilisant l'UpdateFunctionConfigurationaction associée au SnapStartparamètre.
2. Publiez une version de fonction avec l'PublishVersionaction. Lambda initialise votre code, crée un instantané de l'environnement d'exécution initialisé, puis met en cache l'instantané pour un accès à faible latence.

3. Vérifiez qu'elle SnapStart est activée pour la version de la fonction en utilisant l'GetFunctionConfigurationaction. Spécifiez un numéro de version pour confirmer qu' SnapStart il est activé pour cette version. Si la réponse indique que OptimizationStatusc'est le cas 0n et que State est activéActive, SnapStart il est activé et un instantané est disponible pour la version de fonction spécifiée.

```
"SnapStart": {
        "ApplyOn": "PublishedVersions",
        "OptimizationStatus": "On"
    },
    "State": "Active",
```

4. Invoquez la version de la fonction avec l'action Invoke.

États des fonctions Lambda SnapStart et Event

Les états de fonction suivants peuvent se produire lorsque vous utilisez SnapStart.

En attente

Lambda initialise votre code et prend un instantané de l'environnement d'exécution initialisé. Toutes les invocations ou autres actions d'API qui opèrent sur la version de la fonction échouent.

Actif

La création de l'instantané est terminée et vous pouvez invoquer la fonction. Pour l'utiliser SnapStart, vous devez invoquer la version publiée de la fonction, et non la version non publiée ($LATEST).

Inactif

L'état `Inactive` peut se produire lorsque Lambda régénère périodiquement des instantanés de fonction pour appliquer des mises à jour logicielles. Dans ce cas, si votre fonction ne parvient pas à s'initialiser, elle peut entrer dans un état `Inactive`.

Pour les fonctions utilisant un environnement d'exécution Java, Lambda supprime les instantanés au bout de 14 jours sans invocation. Si vous invoquez la version de la fonction après 14 jours, Lambda renvoie une réponse `SnapStartNotReadyException` et commence à initialiser un nouvel instantané. Attendez que la fonction version atteigne l'état `Active`, puis invoquez-la à nouveau.

Échec

Lambda a rencontré une erreur lors de l'exécution du code d'initialisation ou de la création de l'instantané.

Mise à jour d'un instantané

Lambda crée un instantané pour chaque version de fonction publiée. Pour mettre à jour un instantané, publiez une nouvelle version de la fonction.

Utilisation SnapStart avec AWS Kits SDK

Pour effectuer des appels au AWS SDK depuis votre fonction, Lambda génère un ensemble éphémère d'informations d'identification en assumant le rôle d'exécution de votre fonction. Ces informations d'identification sont disponibles en tant que variables d'environnement lors de l'invocation de votre fonction. Vous n'avez pas besoin de fournir des informations d'identification pour le kit SDK directement dans le code. Par défaut, la chaîne de fournisseurs d'informations d'identification vérifie séquentiellement chaque endroit où vous pouvez définir des informations d'identification et sélectionne le premier disponible, généralement les variables d'environnement (`AWS_ACCESS_KEY_ID`, `AWS_SECRET_ACCESS_KEY` et `AWS_SESSION_TOKEN`).

> **Note**
>
> Lorsqu'il SnapStart est activé, le moteur d'exécution Lambda utilise automatiquement les informations d'identification du conteneur (`AWS_CONTAINER_CREDENTIALS_FULL_URI`et`AWS_CONTAINER_AUTHORIZATION_TOKEN`) au lieu des variables d'environnement de la clé d'accès. Cela évite que les informations d'identification n'expirent avant la restauration de la fonction.

Utilisation SnapStart avec CloudFormation, AWS SAM, et AWS CDK

- AWS CloudFormation: Déclarez l'SnapStartentité dans votre modèle.
- AWS Serverless Application Model (AWS SAM) : Déclarez la SnapStartpropriété dans votre modèle.
- Cloud Development Kit AWS (AWS CDK): Utilisez le SnapStartPropertytype.

Suppression d’instantanés

Lambda supprime les instantanés lorsque :

- Vous supprimez la fonction ou la version de la fonction.
- Exécutions Java uniquement : vous n’invoquez pas la version de la fonction pendant 14 jours. Après 14 jours sans invocation, la version de fonction passe à l’état Inactif. Si vous invoquez la version de la fonction après 14 jours, Lambda renvoie une réponse `SnapStartNotReadyException` et commence à initialiser un nouvel instantané. Attendez que la version de la fonction atteigne l’état Actif, puis invoquez-la à nouveau.

Lambda supprime toutes les ressources associées aux instantanés supprimés, conformément au Règlement général sur la protection des données (RGPD).

Gérer l'unicité avec Lambda SnapStart

Lorsque les invocations augmentent sur une SnapStart fonction, Lambda utilise un seul instantané initialisé pour reprendre plusieurs environnements d'exécution. Si votre code d'initialisation génère un contenu unique qui est inclus dans l'instantané, ce contenu peut ne pas être unique lorsqu'il est réutilisé dans plusieurs environnements d'exécution. Pour conserver l'unicité lors de l'utilisation SnapStart, vous devez générer un contenu unique après l'initialisation. Cela inclut les identifiants uniques, les secrets uniques et l'entropie utilisée pour générer un pseudo aléatoire.

Nous vous recommandons les bonnes pratiques suivantes pour vous aider à maintenir l'unicité de votre code. Pour les fonctions Java, Lambda fournit également un outil d'SnapStart analyse open source pour aider à vérifier le code qui suppose un caractère unique. Si vous générez des données uniques pendant la phase d'initialisation, vous pouvez utiliser un hook d'exécution pour rétablir l'unicité. Avec les hooks d'exécution, vous pouvez exécuter un code spécifique immédiatement avant que Lambda ne prenne un instantané ou immédiatement après que Lambda ait repris une fonction à partir d'un instantané.

Évitez de sauvegarder un état qui dépend de l'unicité pendant l'initialisation

Pendant la phase d'initialisation de votre fonction d'événement, évitez de mettre en cache des données censées être uniques, par exemple en générant un identifiant unique pour la journalisation ou en définissant des valeurs de départ pour des fonctions aléatoires. Nous vous recommandons plutôt de générer des données uniques ou de configurer des seeds pour des fonctions random dans votre gestionnaire de fonction ou d'utiliser un hook d'exécution.

Les exemples suivants montrent comment générer un UUID dans le gestionnaire Event Function.

Java

Example— Génération d'un identifiant unique dans le gestionnaire de fonctions d'événement

```
import java.util.UUID;
  public class Handler implements RequestHandler<String, String> {
    private static UUID uniqueSandboxId = null;
    @Override
    public String handleRequest(String event, Context context) {
      if (uniqueSandboxId == null)
        uniqueSandboxId = UUID.randomUUID();
      System.out.println("Unique Sandbox Id: " + uniqueSandboxId);
      return "Hello, World!";
```

```
    }
  }
```

Python

Example— Génération d'un identifiant unique dans le gestionnaire de fonctions d'événement

```
import json
import random
import time

unique_number = None

def lambda_handler(event, context):
    seed = int(time.time() * 1000)
    random.seed(seed)
    global unique_number
    if not unique_number:
        unique_number = random.randint(1, 10000)

    print("Unique number: ", unique_number)

    return "Hello, World!"
```

.NET

Example— Génération d'un identifiant unique dans le gestionnaire de fonctions d'événement

```
namespace Example;
public class SnapstartExample
{
    private Guid _myExecutionEnvironmentGuid;
    public SnapstartExample()
    {
        // This GUID is set for non-restore use cases, such as testing or if
 SnapStart is turned off
        _myExecutionEnvironmentGuid = new Guid();
        // Register the method which will run after each restore. You may need to
 update Amazon.Lambda.Core to see this
        Amazon.Lambda.Core.SnapshotRestore.RegisterAfterRestore(MyAfterRestore);
    }
```

```
    private ValueTask MyAfterRestore()
    {
        // After restoring this snapshot to a new execution environment, update the
 GUID
        _myExecutionEnvironmentGuid = new Guid();
        return ValueTask.CompletedTask;
    }

    public string Handler()
    {
        return $"Hello World! My Execution Environment GUID is
 {_myExecutionEnvironmentGuid}";
    }
}
```

Utilisation de générateurs de nombres pseudo aléatoires cryptographiquement sécurisés (CSPRNG)

Lorsqu'il SnapStart est activé, Lambda prend un instantané de l'environnement d'exécution de votre fonction, y compris de toute la mémoire de l'application et du système. Cela signifie que l'état interne de chaque générateur de nombres aléatoires (RNG) est préservé exactement tel qu'il était au moment de la capture d'écran, ainsi que tous les octets aléatoires que votre application ou ses dépendances ont déjà générés et stockés dans des mémoires tampons.

Lorsque Lambda restaure un environnement d'exécution à partir d'un instantané, il réinitialise le générateur de nombres aléatoires du noyau à partir `/dev/random` et `/dev/urandom` avec une nouvelle entropie. Un logiciel qui lit des nombres aléatoires directement à partir de ces appareils maintient le caractère aléatoire avec SnapStart.

Si votre application dépend du caractère aléatoire, nous vous recommandons d’utiliser des générateurs de nombres aléatoires cryptographiquement sécurisés (CSPRNG). Outre l'OpenSSL fourni par AL, les environnements d'exécution gérés par Lambda compatibles SnapStart (Java version 11+, Python version 3.12+ et .NET version 8+) incluent les CSPRNG intégrés suivants :

- Java : `java.security.SecureRandom`
- Python : `random.SystemRandom`
- .NET : `System.Security.Cryptography.RandomNumberGenerator`

> **Note**
>
> Pour l'exécution de Go Lambda, aucune modification n'est requise si vos fonctions utilisent la bibliothèque standard`crypto/rand`, qui est compatible avec Snapstart par défaut.

Lorsque vous empaquetez votre fonction sous forme d'image de conteneur, votre image de base détermine l'unicité de la compatibilité avec SnapStart :

- Une image de base Lambda pour un environnement d'exécution géré (Java version 11+, Python version 3.12+ et .NET version 8+) — Compatible avec les versions décrites ci-dessus. SnapStart
- L'image de base .al2023 fournie : compatible si l'environnement d'exécution de votre langage de programmation obtient de l'entropie à partir de `/dev/random` ou de la version d'OpenSSL (SnapStart-compatible openssl-snapsafe-libs) répertoriée dans la liste des packages Amazon Linux 2023. `/dev/urandom` Si votre environnement d'exécution repose sur d'autres sources d'entropie, suivez les étapes décrites dans la section « Votre propre image de base » ci-dessous.
- Votre propre image de base : auditez vos bibliothèques cryptographiques et utilisez un hook d'exécution après restauration pour supprimer tout état du générateur de nombres aléatoires (RNG) mis en cache ou les octets aléatoires mis en mémoire tampon, afin de garantir que la bibliothèque lit la nouvelle entropie du système après la restauration. Par exemple, les fonctions Rust utilisées `rand::rngs::ThreadRng` doivent être appelées `reseed()` après la restauration. Nous vous recommandons de créer à l'aide d'une image de base Lambda dans la mesure du possible. En particulier, si votre image de base inclut sa propre version d'OpenSSL ou un fork d'OpenSSL (tel que BoringSSL ou LibreSSL), passez à l'image de base .al2023 fournie, qui inclut une version d'OpenSSL (openssl-snapsafe-libs), ou utilisez libcrypto (-LC). SnapStart-compatible AWSAWS

Versions de bibliothèque minimales prises en charge

AWS les bibliothèques de cryptographie conservent automatiquement le caractère aléatoire en SnapStart commençant par les versions minimales spécifiées dans le tableau suivant. Si vous utilisez ces bibliothèques avec vos fonctions d'événement Lambda, assurez-vous d'utiliser les versions minimales ou ultérieures suivantes :

Bibliothèque	Version minimale prise en charge (x86)	Version minimale prise en charge (ARM)
AWS libcrypto (AWS-LC)	1.16.0	1.30.0
AWS libcrypto FIPS	2.0.13	2.0.13

Si vous empaquetez les bibliothèques cryptographiques précédentes avec vos fonctions d'événement Lambda sous forme de dépendances transitives via les bibliothèques suivantes, assurez-vous d'utiliser les versions minimales suivantes ou des versions ultérieures :

Bibliothèque	Version minimale prise en charge (x86)	Version minimale prise en charge (ARM)
AWS SDK for Java 2.x	2,23,20	2,26,12
AWS Common Runtime pour Java	0,29,8	0,29,25
Amazon Corretto Crypto Provider	2.4.1	2.4.1
Amazon Corretto Crypto Provider FIPS	2.4.1	2.4.1

Les exemples suivants montrent comment utiliser de CSPRNG pour garantir des séquences de nombres uniques même lorsque la fonction est restaurée à partir d'un instantané.

Java

Example— java.security. SecureRandom

```
import java.security.SecureRandom;
  public class Handler implements RequestHandler<String, String> {
    private static SecureRandom rng = new SecureRandom();
    @Override
    public String handleRequest(String event, Context context) {
      for (int i = 0; i < 10; i++) {
```

```
        System.out.println(rng.next());
      }
      return "Hello, World!";
    }
  }
```

Python

Example— aléatoire. SystemRandom

```
import json
import random

secure_rng = random.SystemRandom()

def lambda_handler(event, context):
    random_numbers = [secure_rng.random() for _ in range(10)]

    for number in random_numbers:
        print(number)

    return "Hello, World!"
```

.NET

Example– RandomNumberGenerator

```
using Amazon.Lambda.Core;
using System.Security.Cryptography;
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSeriali

namespace DotnetSecureRandom;

public class Function
{
    public string FunctionHandler()
    {
        using (RandomNumberGenerator rng = RandomNumberGenerator.Create())
        {
            byte[] randomUnsignedInteger32Bytes = new byte[4];
            for (int i = 0; i < 10; i++)
            {
```

```
                rng.GetBytes(randomUnsignedInteger32Bytes);
                int randomInt32 = BitConverter.ToInt32(randomUnsignedInteger32Bytes,
 0);
                Console.WriteLine("{0:G}", randomInt32);
            }
        }
        return "Hello World!";
    }
}
```

SnapStart outil de numérisation (Java uniquement)

Lambda fournit un outil d'analyse pour Java pour vous aider à vérifier le code qui suppose l'unicité. L'outil de SnapStart numérisation est un SpotBugsplugin open source qui exécute une analyse statique par rapport à un ensemble de règles. L'outil d'analyse aide à identifier les implémentations de code potentielles qui pourraient enfreindre les suppositions concernant l'unicité. Pour les instructions d'installation et la liste des vérifications effectuées par l'outil d'analyse, consultez le référentiel aws-lambda-snapstart-java-rules sur. GitHub

Pour en savoir plus sur la gestion de l'unicité avec SnapStart, consultez Starting up faster with AWS Lambda SnapStart sur le blog AWS Compute.

Implémenter le code avant ou après les instantanés de la fonction d'événement Lambda

Vous pouvez utiliser des hooks d'exécution pour implémenter du code avant que Lambda ne crée un instantané ou après que Lambda ait repris une fonction à partir d'un instantané. Les hooks d'exécution sont utiles à diverses fins, telles que :

- Le nettoyage et l'initialisation : avant de créer un instantané, vous pouvez utiliser un hook d'exécution pour effectuer des opérations de nettoyage ou de libération de ressources. Après la restauration d'un instantané, vous pouvez utiliser un hook d'exécution pour réinitialiser les ressources ou les états qui n'ont pas été capturés dans l'instantané.
- La configuration dynamique : vous pouvez utiliser des hooks d'exécution pour mettre à jour dynamiquement la configuration ou d'autres métadonnées avant la création d'un instantané ou après sa restauration. Cela peut être utile si votre fonction doit s'adapter aux modifications de l'environnement d'exécution.
- Les intégrations externes : vous pouvez utiliser des hooks d'exécution pour intégrer des services ou des systèmes externes, tels que l'envoi de notifications ou la mise à jour de l'état externe, dans le cadre du processus de point de contrôle et de restauration.
- L'optimisation des performances : vous pouvez utiliser des hooks d'exécution pour optimiser la séquence de démarrage de votre fonction, par exemple en préchargeant les dépendances. Pour plus d'informations, consultez Personnalisation de performances.

Les pages suivantes expliquent comment implémenter des hooks d'exécution pour votre environnement d'exécution préféré.

Rubriques

- Hooks d' SnapStart exécution Lambda pour Java
- Hooks d'exécution Lambda SnapStart pour Python
- Hooks d' SnapStart exécution Lambda pour .NET
- SnapStart Implémentation de crochets pour les images de conteneurs

Hooks d' SnapStart exécution Lambda pour Java

Vous pouvez utiliser des hooks d'exécution pour implémenter du code avant que Lambda ne crée un instantané ou après que Lambda reprenne une fonction d'événement à partir d'un instantané.

Les hooks d'exécution sont disponibles dans le cadre du projet open source Coordinated Restore at Checkpoint (CRaC). CRaC est en cours de développement pour l'Open Java Development Kit (OpenJDK). Pour un exemple d'utilisation de CRac avec une application de référence, consultez le référentiel CRac sur. GitHub CRaC utilise trois éléments principaux :

- `Resource` – Une interface avec deux méthodes, `beforeCheckpoint()` et `afterRestore()`. Utilisez ces méthodes pour implémenter le code que vous voulez exécuter avant un instantané et après une restauration.
- `Context <R extends Resource>` – Pour recevoir des notifications pour les points de contrôle et les restaurations, une `Resource` doit être enregistrée avec un `Context`.
- `Core`— Le service de coordination, qui fournit le global par défaut par le `Context` biais de la méthode statique`Core.getGlobalContext()`.

Pour plus d'informations sur `Context` et `Resource`, consultez Package org.crac dans la documentation de CRaC.

Suivez les étapes suivantes pour implémenter des hooks d'exécution avec le package org.crac. L'environnement d'exécution Lambda contient une implémentation de contexte CRaC personnalisée qui appelle vos hooks d'exécution avant le point de contrôle et après la restauration.

Enregistrement et exécution du hook d'exécution

L'ordre dans lequel Lambda exécute vos hooks d'exécution est déterminé par l'ordre d'enregistrement. L'ordre d'enregistrement suit l'ordre d'importation, de définition ou d'exécution dans votre code.

- `beforeCheckpoint()` : exécutés dans l'ordre inverse de l'enregistrement
- `afterRestore()` : exécutés dans l'ordre d'enregistrement

Assurez-vous que tous les hooks enregistrés sont correctement importés et inclus dans le code de votre fonction. Si vous enregistrez les hooks d'exécution dans un fichier ou un module distinct, vous devez vous assurer que le module est importé, soit directement, soit dans le cadre d'un package plus large, dans le fichier de gestionnaire de votre fonction. Si le fichier ou le module n'est pas importé dans le gestionnaire de fonctions, Lambda ignore les hooks d'exécution.

> **Note**
>
> Lorsque Lambda crée un instantané, votre code d'initialisation peut s'exécuter jusqu'à 15 minutes. Le délai d'attente est de 130 secondes ou le délai d'expiration de la fonction configurée (900 secondes au maximum), la valeur la plus élevée étant retenue. Vos hooks d'exécution `beforeCheckpoint()` sont comptabilisés dans le délai d'attente du code d'initialisation. Lorsque Lambda restaure un instantané, l'exécution doit se charger et les hooks d'exécution `afterRestore()` doivent se terminer dans le délai imparti (10 secondes). Sinon, vous obtiendrez un SnapStartTimeoutException.

Étape 1 : mettre à jour de configuration de création

Ajoutez la dépendance `org.crac` à la configuration de compilation. L'exemple suivant utilise Gradle. Pour des exemples concernant d'autres systèmes de compilation, consultez la documentation Apache Maven.

```
dependencies {
    compile group: 'com.amazonaws', name: 'aws-lambda-java-core', version: '1.2.1'
    # All other project dependecies go here:
    # ...
    # Then, add the org.crac dependency:
 implementation group: 'org.crac', name: 'crac', version: '1.4.0'
}
```

Étape 2 : mettre à jour le gestionnaire Lambda

Le gestionnaire de fonctions d'événement Lambda est la méthode de votre code de fonction qui traite les événements. Lorsque votre fonction est invoquée, Lambda exécute la méthode du gestionnaire. Votre fonction s'exécute jusqu'à ce que le gestionnaire renvoie une réponse, se ferme ou expire.

Pour plus d'informations, consultez Définir le gestionnaire de fonctions d'événement Lambda en Java.

L'exemple de gestionnaire suivant montre comment exécuter le code avant le point de contrôle (`beforeCheckpoint()`) et après la restauration (`afterRestore()`). Ce gestionnaire enregistre également la `Resource` dans le `Context` global géré par l'environnement d'exécution.

> **Note**
>
> Lorsque Lambda crée un instantané, votre code d'initialisation peut s'exécuter jusqu'à 15 minutes. Le délai d'attente est de 130 secondes ou le délai d'expiration de la fonction configurée (900 secondes au maximum), la valeur la plus élevée étant retenue. Vos hooks d'exécution `beforeCheckpoint()` sont comptabilisés dans le délai d'attente du code d'initialisation. Lorsque Lambda restaure un instantané, l'exécution (JVM) doit se charger et les hooks d'exécution `afterRestore()` doivent se terminer dans le délai imparti (10 secondes). Sinon, vous obtiendrez un SnapStartTimeoutException.

```
...
  import org.crac.Resource;
  import org.crac.Core;
  ...
public class CRaCDemo implements RequestStreamHandler, Resource {
    public CRaCDemo() {
      Core.getGlobalContext().register(this);
    }
    public String handleRequest(String name, Context context) throws IOException {
      System.out.println("Handler execution");
      return "Hello " + name;
    }
    @Override
    public void beforeCheckpoint(org.crac.Context<? extends Resource> context)
        throws Exception {
      System.out.println("Before checkpoint");
    }
    @Override
    public void afterRestore(org.crac.Context<? extends Resource> context)
        throws Exception {
      System.out.println("After restore");
```

`Context` maintient uniquement une `WeakReference` à l'objet enregistré. Si une `Resource` est récupérée par le récupérateur de mémoire, les hooks d'exécution ne s'exécutent pas. Votre code doit maintenir une référence forte à la `Resource` pour garantir l'exécution du hook d'exécution.

Voici deux exemples de modèles à éviter :

Example– Objet sans référence forte

```
Core.getGlobalContext().register( new MyResource() );
```

Example– Objets de classes anonymes

```
Core.getGlobalContext().register( new Resource() {

   @Override
   public void afterRestore(Context<? extends Resource> context) throws Exception {
    // ...
   }

   @Override
   public void beforeCheckpoint(Context<? extends Resource> context) throws Exception {
    // ...
   }

} );
```

Au lieu de cela, maintenez une référence forte. Dans l'exemple suivant, la ressource enregistrée n'est pas récupérée par le récupérateur de mémoire et les hooks d'exécution s'exécutent de manière cohérente.

Example– Objet avec une référence forte

```
Resource myResource = new MyResource(); // This reference must be maintained to prevent
 the registered resource from being garbage collected
Core.getGlobalContext().register( myResource );
```

Hooks d'exécution Lambda SnapStart pour Python

Vous pouvez utiliser des hooks d'exécution pour implémenter du code avant que Lambda ne crée un instantané ou après que Lambda ait repris une fonction à partir d'un instantané. Les hooks d'exécution Python sont disponibles dans le cadre de la bibliothèque Snapshot Restore for Python open source, qui est incluse dans les environnements d'exécution gérés par Python. Cette bibliothèque fournit deux décorateurs que vous pouvez utiliser pour définir vos hooks d'exécution :

- `@register_before_snapshot` : pour les fonctions que vous souhaitez exécuter avant que Lambda ne crée un instantané.

- `@register_after_restore` : pour les fonctions que vous souhaitez exécuter lorsque Lambda reprend une fonction à partir d'un instantané.

Vous pouvez également utiliser les méthodes suivantes afin d'enregistrer des fonctions pouvant être appelées pour des hooks d'exécution :

- `register_before_snapshot(func, *args, **kwargs)`
- `register_after_restore(func, *args, **kwargs)`

Enregistrement et exécution du hook d'exécution

L'ordre dans lequel Lambda exécute vos hooks d'exécution est déterminé par l'ordre d'enregistrement :

- Avant l'instantané : exécutés dans l'ordre inverse de l'enregistrement
- Après l'instantané : exécutés dans l'ordre d'enregistrement

L'ordre d'enregistrement des hooks d'exécution dépend de la façon dont vous définissez les hooks. Lorsque vous utilisez des décorateurs (`@register_before_snapshot` et `@register_after_restore`), l'ordre d'enregistrement suit l'ordre d'importation, de définition ou d'exécution dans votre code. Si vous avez besoin de plus de contrôle sur l'ordre d'enregistrement, utilisez les méthodes `register_before_snapshot()` et `register_after_restore()` au lieu des décorateurs.

Assurez-vous que tous les hooks enregistrés sont correctement importés et inclus dans le code de votre fonction. Si vous enregistrez les hooks d'exécution dans un fichier ou un module distinct, vous devez vous assurer que le module est importé, soit directement, soit dans le cadre d'un package plus large, dans le fichier de gestionnaire de votre fonction. Si le fichier ou le module n'est pas importé dans le gestionnaire de fonctions, Lambda ignore les hooks d'exécution.

> **Note**
>
> Lorsque Lambda crée un instantané, votre code d'initialisation peut s'exécuter jusqu'à 15 minutes. Le délai d'attente est de 130 secondes ou le délai d'expiration de la fonction configurée (900 secondes au maximum), la valeur la plus élevée étant retenue. Vos hooks d'exécution `@register_before_snapshot` sont comptabilisés dans le délai d'attente du code d'initialisation. Lorsque Lambda restaure un instantané, l'exécution doit se charger et les

hooks d'exécution `@register_after_restore` doivent se terminer dans le délai imparti (10 secondes). Sinon, vous obtiendrez une SnapStartTimeoutException.

Exemple

L'exemple de gestionnaire suivant montre comment exécuter le code avant le point de contrôle (`@register_before_snapshot`) et après la restauration (`@register_after_restore`).

```
from snapshot_restore_py import register_before_snapshot, register_after_restore

def lambda_handler(event, context):
    # Handler code

@register_before_snapshot
def before_checkpoint():
    # Logic to be executed before taking snapshots

@register_after_restore
def after_restore():
    # Logic to be executed after restore
```

Pour plus d'exemples, consultez Snapshot Restore pour Python dans le référentiel GitHub AWS.

Hooks d' SnapStart exécution Lambda pour .NET

Vous pouvez utiliser des hooks d'exécution pour implémenter du code avant que Lambda ne crée un instantané ou après que Lambda reprenne une fonction d'événement à partir d'un instantané. Les hooks d'exécution .NET sont disponibles dans le Amazon.Lambda.Corepackage (version 2.5.0 ou ultérieure). Cette bibliothèque fournit deux méthodes que vous pouvez utiliser pour définir vos hooks d'exécution :

- `RegisterBeforeSnapshot()` : code à exécuter avant la création de l'instantané
- `RegisterAfterSnapshot()` : code à exécuter après la reprise d'une fonction à partir d'un instantané

> **Note**
>
> Si vous utilisez le framework Lambda Annotations pour .NET, passez à la Amazon.Lambda.Annotationsversion 1.6.0 ou ultérieure pour garantir la compatibilité avec. SnapStart

Enregistrement et exécution du hook d'exécution

Enregistrez vos hooks dans votre code d'initialisation. Tenez compte des directives suivantes en fonction du modèle d'exécution de votre fonction Lambda :

- Pour l'approche de l'assemblage exécutable, enregistrez vos hooks avant de démarrer l'amorçage Lambda avec `RunAsync`.
- Pour l'approche de la bibliothèque de classes, enregistrez vos hooks dans le constructeur de classe du gestionnaire.
- Pour les applications ASP.NET Core, enregistrez vos hooks avant d'appeler la `WebApplications.Run` méthode.

Pour enregistrer des hooks d'exécution pour SnapStart .NET, utilisez les méthodes suivantes :

```
Amazon.Lambda.Core.SnapshotRestore.RegisterBeforeSnapshot(BeforeCheckpoint);
Amazon.Lambda.Core.SnapshotRestore.RegisterAfterRestore(AfterCheckpoint);
```

Lorsque plusieurs types de hooks sont enregistrés, l'ordre dans lequel Lambda exécute vos hooks d'exécution est déterminé par l'ordre d'enregistrement :

- `RegisterBeforeSnapshot()` : exécutés dans l'ordre inverse de l'enregistrement
- `RegisterAfterSnapshot()` : exécutés dans l'ordre d'enregistrement

> **Note**
>
> Lorsque Lambda crée un instantané, votre code d'initialisation peut s'exécuter jusqu'à 15 minutes. Le délai d'attente est de 130 secondes ou le délai d'expiration de la fonction configurée (900 secondes au maximum), la valeur la plus élevée étant retenue. Vos hooks d'exécution `RegisterBeforeSnapshot()` sont comptabilisés dans le délai d'attente du

code d'initialisation. Lorsque Lambda restaure un instantané, l'exécution doit se charger et les hooks d'exécution `RegisterAfterSnapshot()` doivent se terminer dans le délai imparti (10 secondes). Sinon, vous obtiendrez un SnapStartTimeoutException.

Exemple

L'exemple de fonction suivant montre comment exécuter le code avant le point de contrôle (`RegisterBeforeSnapshot`) et après la restauration (`RegisterAfterRestore`).

```
public class SampleClass
{
    public SampleClass()
    {
        Amazon.Lambda.Core.SnapshotRestore.RegisterBeforeSnapshot(BeforeCheckpoint);
        Amazon.Lambda.Core.SnapshotRestore.RegisterAfterRestore(AfterCheckpoint);
    }

    private ValueTask BeforeCheckpoint()
    {
        // Add logic to be executed before taking the snapshot
        return ValueTask.CompletedTask;
    }

    private ValueTask AfterCheckpoint()
    {
        // Add logic to be executed after restoring the snapshot
        return ValueTask.CompletedTask;
    }

    public APIGatewayProxyResponse FunctionHandler(APIGatewayProxyRequest request,
 ILambdaContext context)
    {
        // Add business logic

        return new APIGatewayProxyResponse
        {
            StatusCode = 200
        };
    }
}
```

SnapStart Implémentation de crochets pour les images de conteneurs

Vue d'ensemble

Lors de l'utilisation SnapStart avec une fonction d'image de conteneur, le moteur d'exécution doit coordonner le cycle de vie de la fonction et invoquer les hooks avant capture et après restauration pendant les phases de cycle de vie appropriées. Ces hooks vous permettent d'exécuter une logique personnalisée (telle que l'actualisation des informations d'identification ou le réensemencement de générateurs de nombres aléatoires) à certains moments du cycle de vie des snapshots et des restaurations. Si vous utilisez un environnement d'exécution géré supporté ou les images de base correspondantes pour ces environnements d'exécution (Java version 11+, Python version 3.12+ et .NET version 8+), Lambda coordonne le cycle de vie pour vous. SnapStart Enregistrez vos hooks via l'API décrite dansImplémenter le code avant ou après les instantanés de la fonction d'événement Lambda.

Si vous utilisez vos propres images de conteneur de base, des clients d'interface d'exécution (RIC) ou les images de base de Lambda pour provided.al2023 ou Ruby Node.js, suivez les étapes de cette page pour les utiliser. SnapStart

Conditions préalables

Lorsque Lambda restaure une fonction à partir d'un instantané, tout état défini lors de l'initialisation, tel que les générateurs de nombres aléatoires, les identifiants uniques et les informations d'identification mises en cache, est partagé dans tous les environnements d'exécution restaurés à partir de cet instantané. Avant de l'utiliser SnapStart avec votre fonction d'événement Lambda basée sur une image de conteneur, vérifiez Gérer l'unicité avec Lambda SnapStart et assurez-vous que les exigences décrites dans Utiliser des générateurs de nombres pseudoaléatoires (CSPRNG) sécurisés par chiffrement sont respectées.

Après avoir vérifié que les exigences sont satisfaites, choisissez l'une des deux options suivantes :

1. Option 1 : Si vous avez besoin de crochets avant et après restauration pour exécuter une logique personnalisée lorsque le snapshot de votre fonction est repris, suivez les instructions de la section. Mettre en œuvre SnapStart des hooks de cycle
2. Option 2 : Si vous n'avez pas besoin de ces hooks, activez cette image SnapStart de conteneur en spécifiant l'étiquette suivante dans votre Dockerfile :

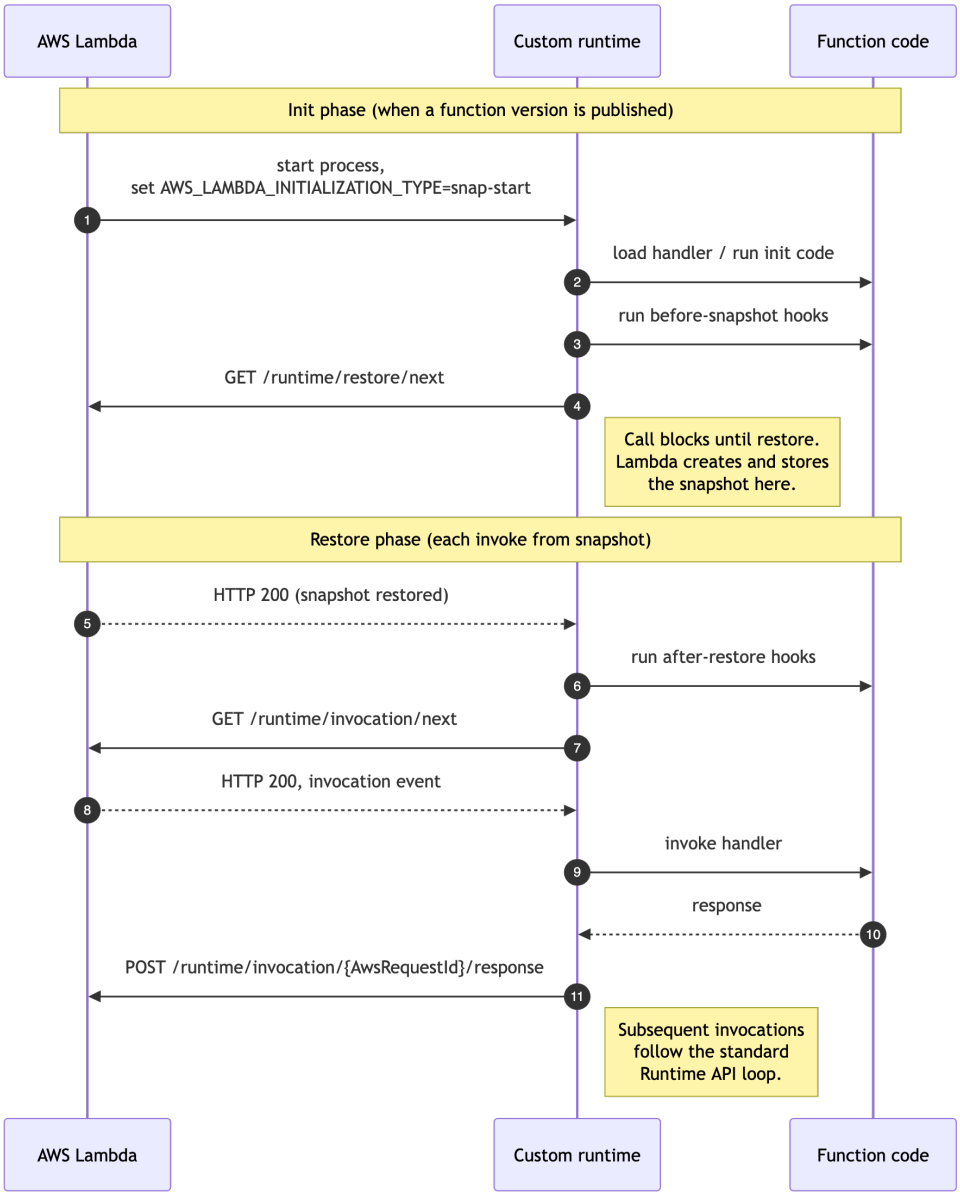
```
LABEL com.amazonaws.lambda.feature.snapstart="Allow"
```

Si votre image de conteneur n'implémente pas l'`/restore/next`API et n'inclut pas l'étiquette, la publication de la version échouera.

> **Note**
>
> Ces prérequis ne sont pas obligatoires si vous utilisez des images de base gérées par Lambda pour Java (version 11+), Python (version 3.12+) et .NET (version 8+) car elles coordonnent SnapStart déjà le cycle de vie et répondent aux exigences d'unicité.

Aperçu du cycle de vie

Le schéma suivant montre l'ordre des appels d'API Runtime qu'un environnement d'exécution SnapStart personnalisé est censé effectuer. Tous les appels font partie du contrat d'API Runtime, tandis que les appels #3, #4, #5 et #6 sont spécifiques à SnapStart.



Mettre en œuvre SnapStart des hooks de cycle

Pour utiliser SnapStart les fonctions d'image de votre conteneur, suivez les étapes ci-dessous :

1. Exécutez les hooks avant l'instantané et déclenchez le processus de capture d'écran : comme dernière étape du code d'initialisation de votre fonction, exécutez les crochets avant l'instantané si nécessaire et déclenchez le processus de capture d'écran. Effectuez ces étapes uniquement si cette option SnapStart est activée, en vérifiant que la valeur de la variable d'`AWS_LAMBDA_INITIALIZATION_TYPE`environnement est définie sur`snap-start`. Exécutez vos hooks enregistrés avant la capture d'écran, puis appelez `GET /runtime/restore/next` pour déclencher le processus de capture instantanée. Si un hook antérieur à la capture d'écran

génère ou renvoie une erreur, le moteur d'exécution publie l'erreur sur le point de terminaison. `/runtime/init/error` Consultez l'exemple de pseudo-code ci-dessous :

```
# After all initialization code has finished:

   READ initialization_type FROM environment variable
 "AWS_LAMBDA_INITIALIZATION_TYPE"

   IF initialization_type IS "snap-start" THEN

       TRY
           EXECUTE registered before-snapshot hooks
       ON ERROR
           POST error to /runtime/init/error
               SET header  Lambda-Runtime-Function-Error-Type  TO
 <Category.Reason>
               SET body    TO  { errorMessage, errorType, stackTrace }
           EXIT process with non-zero code

       # Signal readiness for snapshot
       SEND GET request to /runtime/restore/next
       # The request blocks until Lambda restores the execution environment from
 the snapshot, then returns HTTP 200.

   END IF
```

> **Note**
>
> La phase d'initialisation et les hooks précédant la capture d'écran partagent un délai d'expiration combiné de. `max(function_timeout, 130 seconds)` Si cette limite est dépassée, Lambda échoue à la PublishVersion demande. De plus`/runtime/invocation/next`, un `/runtime/restore/next` appel est un appel bloquant. Il bloque jusqu'à ce que Lambda restaure l'environnement d'exécution à partir du snapshot.

2. Exécutez les hooks après la restauration, puis entrez dans la boucle d'appel. Lorsque `GET /runtime/restore/next` renvoie 200, votre environnement d'exécution doit exécuter tous les hooks enregistrés après restauration avant de passer à la boucle d'appel. Si un hook après restauration échoue, signalez l'erreur à`/runtime/restore/error`. Une fois les hooks après restauration terminés, entrez dans la boucle d'appel standard en appelant`GET /runtime/`

`invocation/next`. À partir de ce moment, le comportement est identique à celui d'une fonction qui n'utilise pas SnapStart. Consultez l'exemple de pseudo-code ci-dessous :

```
# After the snapshot has been restored
# (i.e., GET /runtime/restore/next has returned HTTP 200):

    TRY
        EXECUTE registered after-restore hooks
    ON ERROR
        POST error to /runtime/restore/error
            SET header  Lambda-Runtime-Function-Error-Type  TO  <Category.Reason>
            SET body    TO  { errorMessage, errorType, stackTrace }

# Proceed to the invoke loop
       GET /runtime/invocation/next
```

Gestion des erreurs

Si un hook échoue, le moteur d'exécution doit signaler l'erreur au point de terminaison d'API approprié et quitter le processus. Le tableau ci-dessous résume le comportement de chaque phase :

Phase	Erreur : point de terminaison API	Que se passe-t-il en cas d'échec
Initialiser/ avant-instantané	`POST /runtime/init/error`	Lambda échoue à la demande. PublishVersion Quittez le processus.
After-restore	`POST /runtime/restore/error`	Lambda échoue à l'invocation en vol et détruit l'environnement d'exécution. Quittez le processus.

Pour les deux points de terminaison de l'API, définissez l'`Lambda-Runtime-Function-Error-Type`en-tête sur une valeur au format `<Category.Reason>` (par exemple, `Runtime.BeforeSnapshotError` ou`Runtime.AfterRestoreError`). Incluez un corps d'erreur avec `errorMessage`e`errorType`, et un élément facultatif`stackTrace`.

Pour la spécification complète des points de terminaison de l'API et les codes de réponse, consultez Erreur d'initialisation et Erreur de restauration (applicable uniquement pour SnapStart) dans la référence de l'API Runtime.

Surveillance pour Lambda SnapStart

Vous pouvez surveiller vos SnapStart fonctions Lambda à l'aide d'Amazon CloudWatch, AWS X-Ray, et du. Accès aux données de télémétrie en temps réel pour les extensions à l'aide de l'API de télémétrie

> **Note**
>
> Les variables `AWS_LAMBDA_LOG_GROUP_NAME` d'`AWS_LAMBDA_LOG_STREAM_NAME`environnement et ne sont pas disponibles dans les fonctions Lambda SnapStart .

Comprendre le comportement de journalisation et de facturation avec SnapStart

Le format du flux de CloudWatch log pour les SnapStart fonctions présente quelques différences :

- Journaux d'initialisation – Lorsqu'un nouvel environnement d'exécution est créé, le `REPORT` n'inclut pas le champ `Init Duration`. C'est parce que Lambda initialise les SnapStart fonctions lorsque vous créez une version plutôt que lors de l'appel de fonctions. Pour SnapStart les fonctions, le `Init Duration` champ se trouve dans l'`INIT_REPORT`enregistrement. Cet enregistrement indique les détails de la durée du Phase d'initialisation, y compris la durée de tout hook d'exécution `beforeCheckpoint`.
- Journaux d'invocation – Lorsqu'un nouvel environnement d'exécution est créé, le `REPORT` inclut les champs `Restore Duration` et `Billed Restore Duration` :
  - `Restore Duration` : le temps nécessaire à Lambda pour restaurer un instantané, charger l'exécution et exécuter les éventuels hooks d'exécution après restauration. Le processus de restauration des instantanés peut inclure du temps consacré à des activités en dehors de la MicroVM. Ce temps est indiqué dans `Restore Duration`.
  - `Billed Restore Duration` : le temps nécessaire à Lambda pour charger l'exécution et exécuter les éventuels hooks d'exécution après restauration.

> **Note**
>
> Comme pour toutes les fonctions d'événement Lambda, des frais de durée s'appliquent au code exécuté dans le gestionnaire de fonctions. Pour les SnapStart fonctions, les frais de durée s'appliquent également au code d'initialisation déclaré en dehors du gestionnaire,

au temps nécessaire au chargement de l'exécution et à tout code exécuté dans un hook d'exécution.

La durée du démarrage à froid est la somme de `Restore Duration` + `Duration`.

L'exemple suivant est une requête Lambda Insights qui renvoie les percentiles de latence pour les fonctions. SnapStart Pour plus d'informations sur les demandes Lambda Insights, consultez Exemple de flux de travail utilisant des requêtes pour résoudre les problèmes liés à une fonction événementielle.

```
filter @type = "REPORT"
  | parse @log /\d+:\/aws\/lambda\/(?<function>.*)/
  | parse @message /Restore Duration: (?<restoreDuration>.*?) ms/
  | stats
count(*) as invocations,
pct(@duration+coalesce(@initDuration,0)+coalesce(restoreDuration,0), 50) as p50,
pct(@duration+coalesce(@initDuration,0)+coalesce(restoreDuration,0), 90) as p90,
pct(@duration+coalesce(@initDuration,0)+coalesce(restoreDuration,0), 99) as p99,
pct(@duration+coalesce(@initDuration,0)+coalesce(restoreDuration,0), 99.9) as p99.9
group by function, (ispresent(@initDuration) or ispresent(restoreDuration)) as
 coldstart
  | sort by coldstart desc
```

X-Ray suivi actif pour SnapStart

Vous pouvez l'utiliser X-Raypour suivre les requêtes adressées aux fonctions Lambda SnapStart . Il existe quelques différences entre les X-Ray sous-segments des SnapStart fonctions :

- Il n'existe aucun `Initialization` sous-segment pour les SnapStart fonctions.
- Le sous-segment `Restore` indique le temps nécessaire à Lambda pour restaurer un instantané, charger l'exécution et exécuter les éventuels hooks d'exécution après restauration. Le processus de restauration des instantanés peut inclure du temps consacré à des activités en dehors de la MicroVM. Cette heure est indiquée dans le sous-segment `Restore`. Le temps passé en dehors de la microVM pour restaurer un instantané ne vous est pas facturé.

Événements de l'API de télémétrie pour SnapStart

Lambda envoie les SnapStart événements suivants au : API de télémétrie

- `Platform.restoRestart` – Indique l'heure à laquelle la phase `Restore` a commencé.
- `platform.restore RuntimeDone` – Indique si la phase `Restore` a réussi. Lambda envoie ce message lorsque l'environnement d'exécution envoie une demande d'API d'exécution `restore/next`. Il existe trois statuts possibles : succès, échec et dépassement de délai.
- `Platform.RestoreReport` – Indique la durée de la phase `Restore` et le nombre de millisecondes pour lesquelles vous avez été facturé pendant cette phase.

Métriques de l'URL de la fonction et de l'Amazon API Gateway

Si vous créez une API Web à l'aide d'API Gateway, vous pouvez utiliser la IntegrationLatencymétrique pour mesurer la latence de bout en bout (le temps entre le moment où API Gateway transmet une demande au backend et le moment où il reçoit une réponse du backend).

Si vous utilisez une URL de fonction Lambda, vous pouvez utiliser la UrlRequestLatencymétrique pour mesurer la latence de bout en bout (le temps entre le moment où l'URL de la fonction reçoit une demande et le moment où l'URL de la fonction renvoie une réponse).

Modèle de sécurité pour Lambda SnapStart

AWS Lambda SnapStart prend en charge le chiffrement au repos. Lambda chiffre les instantanés avec un. AWS KMS key Par défaut, Lambda utilise un. Clé gérée par AWS Si ce comportement par défaut convient à votre flux, vous n'avez pas besoin de configurer autre chose.

Sinon, vous pouvez utiliser l'`--kms-key-arn`option de la commande create-function ou update-function-configuration pour fournir une clé gérée par le client. AWS KMS Vous pouvez procéder ainsi pour contrôler la rotation de la clé KMS ou pour répondre aux exigences de votre organisation en matière de gestion des clés KMS. Les clés gérés par le client entraînent des frais AWS KMS standard. Pour en savoir plus, consultez Pricing AWS Key Management Service (Tarification).

Si votre fonction événementielle est également une fonction durable, la clé gérée par le client qui chiffre les SnapStart instantanés est indépendante de la clé gérée par le client qui chiffre les données d'exécution durables. Pour plus d’informations, consultez Chiffrement AWS Lambda données d'exécution durables.

Lorsque vous supprimez une SnapStart fonction ou une version de fonction, toutes les `Invoke` demandes adressées à cette fonction ou version de fonction échouent. Lambda supprime toutes les ressources associées aux instantanés supprimés, conformément au Règlement général sur la protection des données (RGPD).

Maximisez les performances Lambda SnapStart

Rubriques

- Personnalisation de performances
- Bonnes pratiques concernant le réseau

Personnalisation de performances

Pour optimiser les avantages de SnapStart, tenez compte des recommandations d'optimisation du code suivantes pour votre environnement d'exécution.

> **Note**
>
> SnapStart fonctionne mieux lorsqu'il est utilisé avec des invocations de fonctions à grande échelle. Les fonctions qui sont rarement invoquées peuvent ne pas bénéficier des mêmes améliorations de performance.

Java

Pour optimiser les avantages de SnapStart, nous vous recommandons de précharger les dépendances et d'initialiser les ressources qui contribuent à la latence de démarrage dans votre code d'initialisation plutôt que dans le gestionnaire de fonctions d'événement. Cela permet de déplacer la latence associée au chargement intensif de classes hors du chemin d'invocation, optimisant ainsi les performances de démarrage avec SnapStart.

Si vous ne pouvez pas précharger les dépendances ou les ressources pendant l'initialisation, nous vous recommandons de les précharger avec des invocations fictives. Pour ce faire, mettez à jour le code du gestionnaire de fonctions, comme indiqué dans l'exemple suivant, à partir de la fonction pet store du GitHub référentiel AWS Labs.

```
private static SpringLambdaContainerHandler<AwsProxyRequest, AwsProxyResponse> handler;
  static {
      try {
          handler =
 SpringLambdaContainerHandler.getAwsProxyHandler(PetStoreSpringAppConfig.class);

          // Use the onStartup method of the handler to register the custom filter
```

```
            handler.onStartup(servletContext -> {
                FilterRegistration.Dynamic registration =
servletContext.addFilter("CognitoIdentityFilter", CognitoIdentityFilter.class);
                registration.addMappingForUrlPatterns(EnumSet.of(DispatcherType.REQUEST),
false, "/*");
            });

            // Send a fake Amazon API Gateway request to the handler to load classes
ahead of time
            ApiGatewayRequestIdentity identity = new ApiGatewayRequestIdentity();
            identity.setApiKey("foo");
            identity.setAccountId("foo");
            identity.setAccessKey("foo");

            AwsProxyRequestContext reqCtx = new AwsProxyRequestContext();
            reqCtx.setPath("/pets");
            reqCtx.setStage("default");
            reqCtx.setAuthorizer(null);
            reqCtx.setIdentity(identity);

            AwsProxyRequest req = new AwsProxyRequest();
            req.setHttpMethod("GET");
            req.setPath("/pets");
            req.setBody("");
            req.setRequestContext(reqCtx);

            Context ctx = new TestContext();
            handler.proxy(req, ctx);


        } catch (ContainerInitializationException e) {
            // if we fail here. We re-throw the exception to force another cold start
            e.printStackTrace();
            throw new RuntimeException("Could not initialize Spring framework", e);
        }
    }
```

Python

Pour en tirer le meilleur parti SnapStart, concentrez-vous sur l'organisation efficace du code et la gestion des ressources au sein de vos fonctions Python. De manière générale, effectuez les tâches de calcul intensives pendant la phase d'initialisation. Cette approche élimine les opérations fastidieuses du processus d'invocation, améliorant ainsi les performances globales des fonctions.

Pour implémenter cette stratégie de manière efficace, nous vous recommandons les bonnes pratiques suivantes :

- Importez les dépendances en dehors du gestionnaire de fonction.
- Créez des instances `boto3` en dehors du gestionnaire.
- Initialisez les ressources ou les configurations statiques avant que le gestionnaire ne soit invoqué.
- Envisagez d'utiliser un hook d'exécution avant l'instantané pour les tâches gourmandes en ressources, comme le téléchargement de fichiers externes, le préchargement de frameworks tels que Django ou le chargement de modèles de machine learning.

Example— Optimise la fonction d'événement Python pour SnapStart

```
# Import all dependencies outside of Lambda handler
from snapshot_restore_py import register_before_snapshot
import boto3
import pandas
import pydantic

# Create S3 and SSM clients outside of Lambda handler
s3_client = boto3.client("s3")

# Register the function to be called before snapshot
@register_before_snapshot
def download_llm_models():
    # Download an object from S3 and save to tmp
    # This files will persist in this snapshot
    with open('/tmp/FILE_NAME', 'wb') as f:
        s3_client.download_fileobj('amzn-s3-demo-bucket', 'OBJECT_NAME', f)
    ...

def lambda_handler(event, context):
    ...
```

.NET

Pour réduire le temps de compilation juste à temps (JIT) et de chargement de l'assemblage, pensez à appeler votre gestionnaire de fonctions d'événement à partir d'un hook d'exécution. `RegisterBeforeCheckpoint` En raison du fonctionnement de la compilation hiérarchisée .NET, vous obtiendrez des résultats optimaux en invoquant le gestionnaire plusieurs fois, comme indiqué dans l'exemple suivant.

> **Important**
>
> Assurez-vous que l'invocation de votre fonction fictive ne produit pas d'effets secondaires imprévus, tels que le lancement de transactions commerciales.

Example

```
public class Function
{
    public Function()
    {
        Amazon.Lambda.Core.SnapshotRestore.RegisterBeforeSnapshot(FunctionWarmup);
    }

    // Warmup method that calls the function handler before snapshot to warm up
 the .NET code and runtime.
    // This speeds up future cold starts after restoring from a snapshot.

    private async ValueTask FunctionWarmup()
    {
        var request = new APIGatewayProxyRequest
        {
            Path = "/heathcheck",
            HttpMethod = "GET"
        };

        for (var i = 0; i < 10; i++)
        {
            await FunctionHandler(request, null);
        }
    }

    public async Task<APIGatewayProxyResponse> FunctionHandler(APIGatewayProxyRequest
 request, ILambdaContext context)
    {
        //
        // Process HTTP request
        //

        var response = new APIGatewayProxyResponse
        {
            StatusCode = 200
```

```
        };

        return await Task.FromResult(response);
    }
}
```

Bonnes pratiques concernant le réseau

L'état des connexions que votre fonction d'événement établit pendant la phase d'initialisation n'est pas garanti lorsque Lambda reprend votre fonction à partir d'un instantané. Dans la plupart des cas, les connexions réseau établies par un AWS SDK reprennent automatiquement. Pour les autres connexions, nous vous recommandons les bonnes pratiques suivantes.

Re-establish connexions réseau

Rétablissez toujours vos connexions réseau lorsque votre fonction reprend à partir d'un instantané. Nous vous recommandons de rétablir les connexions réseau dans le gestionnaire de fonction. Vous pouvez également utiliser un hook d'exécution après la restauration.

N'utilisez pas le nom d'hôte comme identifiant unique d'environnement d'exécution

Nous vous déconseillons d'utiliser `hostname` pour identifier votre environnement d'exécution comme un nœud ou un conteneur unique dans vos applications. Avec SnapStart, un seul instantané est utilisé comme état initial pour plusieurs environnements d'exécution. Tous les environnements d'exécution renvoient la même valeur `hostname` pour `InetAddress.getLocalHost()` (Java), `socket.gethostname()` (Python) et `Dns.GetHostName()` (.NET). Pour les applications qui nécessitent une identité ou une valeur `hostname` d'environnement d'exécution unique, nous vous recommandons de générer un identifiant unique dans le gestionnaire de fonction. Ou bien, utilisez un hook d'exécution après la restauration pour générer un ID unique, puis utilisez cet ID unique comme identifiant de l'environnement d'exécution.

Évitez de lier les connexions à des ports source fixes

Nous vous recommandons d'éviter de lier les connexions réseau à des ports source fixes. Les connexions sont rétablies lorsqu'une fonction reprend à partir d'un instantané, et les connexions réseau qui sont liées à un port source fixe peuvent échouer.

Évitez d'utiliser le cache DNS de Java

Les fonctions d'événement Lambda mettent déjà en cache les réponses DNS. Si vous utilisez un autre cache DNS avec SnapStart, vous risquez de rencontrer des délais de connexion lorsque la fonction reprend à partir d'un instantané.

La classe `java.util.logging.Logger` peut activer indirectement le cache DNS de la JVM. Pour remplacer les paramètres par défaut, définissez networkaddress.cache.ttl sur 0 avant de procéder à l'initialisation de `logger`. Exemple :

```
public class MyHandler {
  // first set TTL property
  static{
   java.security.Security.setProperty("networkaddress.cache.ttl" , "0");
  }
 // then instantiate logger
  var logger = org.apache.logging.log4j.LogManager.getLogger(MyHandler.class);
}
```

Pour éviter les échecs `UnknownHostException` de l'environnement d'exécution de Java 11, nous vous recommandons de définir la valeur de `networkaddress.cache.negative.ttl` sur 0. Dans les environnements d'exécution de Java 17 et versions ultérieures, cette étape n'est pas nécessaire. Vous pouvez définir cette propriété pour une fonction d'événement Lambda avec la variable d'`AWS_LAMBDA_JAVA_NETWORKADDRESS_CACHE_NEGATIVE_TTL=0`environnement.

La désactivation du cache DNS de la JVM ne désactive pas la mise en cache DNS gérée par Lambda.

Résolution des SnapStart erreurs liées aux fonctions d'événement Lambda

Cette page aborde les problèmes courants qui se produisent lors de l'utilisation de Lambda SnapStart, notamment les erreurs de création de snapshots, les erreurs de délai d'expiration et les erreurs de service internes.

SnapStartNotReadyException

Erreur : une erreur s'est produite (SnapStartNotReadyException) lors de l'appel de l'opération Invoke20150331 : Lambda initialise votre fonction d'événement. L'invocation sera possible une fois que l'état de votre fonction deviendra ACTIVE.

Causes courantes

Cette erreur se produit lorsque vous essayez d'invoquer une version de fonction qui se trouve à l'état `Inactive`. La version de votre fonction devient `Inactive` lorsqu'elle n'a pas été invoquée depuis 14 jours ou lorsque Lambda recycle périodiquement l'environnement d'exécution.

Résolution

Attendez que la fonction version atteigne l'état `Active`, puis invoquez-la à nouveau.

SnapStartTimeoutException

Problème : vous recevez un `SnapStartTimeoutException` lorsque vous essayez d'invoquer une version de SnapStart fonction.

Cause courante

Pendant la phase de restauration, Lambda restaure l'environnement d'exécution Java et exécute tous les hooks d'exécution après la restauration. Si un hook d'exécution après la restauration s'exécute pendant plus de 10 secondes, la phase `Restore` expire et vous obtenez une erreur lorsque vous essayez d'invoquer la fonction. Les problèmes de connexion réseau et d'identification peuvent également entraîner des délais d'attente de la phase `Restore`.

Résolution

Consultez les CloudWatch journaux de la fonction pour détecter les erreurs de temporisation survenues pendant la phase de restauration. Assurez-vous que tous les hooks après restauration se terminent en moins de 10 secondes.

Example CloudWatch journal

```
{ "cause": "Lambda couldn't restore the snapshot within the timeout limit. (Service:
 Lambda, Status Code: 408, Request ID: 11a222c3-410f-427c-ab22-931d6bcbf4f2)", "error":
 "Lambda.SnapStartTimeoutException"}
```

Erreur interne du service 500

Erreur : Lambda n'a pas pu créer de nouvel instantané car vous avez atteint votre limite de création d'instantanés simultanés.

Cause courante

Une erreur 500 est une erreur interne au sein du service Lambda lui-même, plutôt qu'un problème lié à votre fonction ou à votre code. Ces erreurs sont souvent intermittentes.

Résolution

Réessayez de publier la version de la fonction.

401 Accès non autorisé

Erreur : jeton de session ou clé d'en-tête incorrect

Cause courante

Cette erreur se produit lorsque vous utilisez le magasin de AWS Systems Manager paramètres et l' AWS Secrets Manager extension avec Lambda SnapStart. Lorsque votre fonction l'utilise SnapStart, elle obtient les informations d'identification d'un point de terminaison du conteneur, et Lambda ne définit pas `AWS_SESSION_TOKEN` la variable d'environnement. Si votre fonction définit l'`X-Aws-Parameters-Secrets-Token`en-tête à partir de cette variable d'environnement, l'en-tête est vide et l'extension rejette la demande.

Résolution

Pour corriger cette erreur, utilisez la chaîne du fournisseur d'informations d'identification du AWS SDK pour récupérer le jeton de session au lieu de lire directement la variable d'`AWS_SESSION_TOKEN`environnement. Définissez l'`X-Aws-Parameters-Secrets-Token`en-tête sur le jeton renvoyé par la chaîne de fournisseurs. La chaîne de fournisseurs d'informations d'identification renvoie le jeton de session correct dans tous les modes d'initialisation, y compris. SnapStart Pour obtenir un exemple de code, consultez Utiliser les secrets de Secrets Manager dans Lambda Event Functions.

UnknownHostException (Java)

Erreur : impossible d'exécuter la requête HTTP : le certificat pour `abc.us-east-1.amazonaws.com` ne correspond à aucun des noms alternatifs d'objet.

Cause courante

Les fonctions d'événement Lambda mettent déjà en cache les réponses DNS. Si vous utilisez un autre cache DNS avec SnapStart, vous risquez de rencontrer des délais de connexion lorsque la fonction reprend à partir d'un instantané.

Résolution

Pour éviter les échecs `UnknownHostException` de l'environnement d'exécution de Java 11, nous vous recommandons de définir la valeur de `networkaddress.cache.negative.ttl` sur 0. Dans les environnements d'exécution de Java 17 et versions ultérieures, cette étape n'est pas nécessaire. Vous pouvez définir cette propriété pour une fonction d'événement Lambda avec la variable d'`AWS_LAMBDA_JAVA_NETWORKADDRESS_CACHE_NEGATIVE_TTL=0`environnement.

Échecs de création d'instantanés

Erreur : AWS Lambda impossible d'appeler votre SnapStart fonction. Si cette erreur persiste, consultez les CloudWatch journaux de votre fonction pour détecter les erreurs d'initialisation.

Résolution

Consultez les CloudWatch journaux Amazon de votre fonction pour connaître les délais d'expiration du hook d'exécution avant le point de contrôle. Vous pouvez également essayer de publier une nouvelle version de fonction, ce qui peut parfois résoudre le problème.

Latence de création d'instantanés

Problème : lorsque vous publiez une nouvelle version de fonction, celle-ci reste à l'état `Pending` pendant une longue période.

Cause courante

Lorsque Lambda crée un instantané, votre code d'initialisation peut s'exécuter jusqu'à 15 minutes. Le délai d'attente est de 130 secondes ou le délai d'expiration de la fonction configurée (900 secondes au maximum), la valeur la plus élevée étant retenue.

Si votre fonction est attachée à un VPC, Lambda devra peut-être également créer des interfaces réseau avant que la fonction ne devienne `Active`. Si vous essayez d'invoquer la version de la fonction alors que la fonction est `Pending`, vous pourriez obtenir une erreur 409 `ResourceConflictException`. Si la fonction est invoquée à l'aide d'un point de terminaison Amazon API Gateway, une erreur 500 peut s'afficher dans API Gateway.

Résolution

Attendez au moins 15 minutes que la version de la fonction soit initialisée avant de l'invoquer.

Isolement des locataires

Utilisez le mode d'isolation des locataires lorsque vous avez besoin de traiter des demandes isolées pour des utilisateurs finaux individuels ou des locataires invoquant une fonction d'événement Lambda, auparavant connue sous le nom de fonction Lambda. Cette fonctionnalité simplifie la création d'applications mutualisées qui traitent du code ou des données spécifiques au locataire, telles que les plateformes SaaS pour l'automatisation des flux de travail ou l'exécution de code, en supprimant la nécessité de gérer les ressources fonctionnelles spécifiques au locataire et la logique de routage des demandes.

Multi-tenant les applications sont soumises à des exigences d'isolation strictes lorsqu'elles exécutent du code ou traitent des données pour des locataires individuels ou des utilisateurs finaux. Avec le mode d'isolation des locataires, Lambda utilise un identifiant de locataire spécifié par le client pour acheminer les demandes vers les environnements d'exécution des fonctions sous-jacents, garantissant ainsi que les environnements d'exécution d'une fonction ne sont utilisés que pour traiter les appels provenant de l'utilisateur final ou du locataire spécifié. Les environnements d'exécution des fonctions de Lambda utilisent la virtualisation Firecracker pour isoler les charges de travail.

Lorsqu'une fonction d'événement utilisant le mode d'isolation du locataire reçoit un appel avec un identifiant de locataire, Lambda tente d'abord de localiser un environnement d'exécution disponible associé à cet identifiant de locataire. S'il n'existe aucun environnement d'exécution, Lambda crée et attribue un nouvel environnement d'exécution à ce locataire. À mesure que les invocations de fonctions avec l'identifiant de locataire spécifié augmentent, Lambda localise ou crée de nouveaux environnements d'exécution selon les besoins.

Pour savoir comment utiliser l'isolation des locataires, voirthe section called “Permettre l'isolement des locataires”. Pour plus d'informations sur l'accès au contexte du locataire dans votre code, consultezthe section called “Accès en code”. Pour surveiller les fonctions isolées par les locataires,

voir. the section called “Contrôle” Pour obtenir de l'aide pour résoudre les problèmes, consultezthe section called “Résolution des problèmes”.

Rubriques

- Quand utiliser le mode d'isolation des locataires
- Fonctions prises en charge et limitations
- Pris en charge Régions AWS
- Considérations
- Tarification
- Mode d'isolation
- Activation de l'isolation des locataires pour les fonctions d'événement Lambda
- Invocation de fonctions d'événement Lambda avec isolation des locataires
- Accès à l'identifiant du locataire dans le code Lambda Event Function
- Surveillance des fonctions d'événement Lambda avec isolation des locataires
- Résolution des problèmes d'isolation des locataires pour les fonctions d'événement Lambda

Quand utiliser le mode d'isolation des locataires

Utilisez le mode d'isolation des locataires lorsque vous devez servir plusieurs utilisateurs finaux ou locataires à l'aide d'une seule fonction d'événement Lambda, tout en veillant à ce que les environnements d'exécution utilisés pour traiter les appels destinés à des locataires individuels restent isolés les uns des autres. Cette isolation stricte des environnements d'exécution est requise pour les applications multi-locataires qui :

- Exécuter le code fourni par l'utilisateur final : le maintien d'environnements d'exécution distincts pour les clients individuels peut limiter l'impact de l'exécution de code fourni par l'utilisateur qui peut être incorrect ou malveillant.
- Traitement des données spécifiques au locataire : le maintien d'environnements d'exécution distincts pour chaque locataire peut empêcher l'exposition de données sensibles spécifiques au locataire à d'autres locataires.

Plusieurs demandes d'invocation émanant du même locataire peuvent réutiliser le même environnement d'exécution de fonctions, réduisant ainsi les démarrages à froid et améliorant les temps de réponse pour les applications sensibles à la latence.

Fonctions prises en charge et limitations

Le mode d'isolation du locataire n'est pas pris en charge avec les fonctions d'événement qui utilisent des URL de fonctions, la simultanéité provisionnée ou SnapStartavec les fonctions d'événement qui s'exécutent sur des instances gérées Lambda. Vous pouvez envoyer des demandes à une fonction isolée par le locataire à l'aide d'invocations synchrones, d'invocationsasynchrones ou en utilisant Amazon API Gateway comme déclencheur d'événement.

Pris en charge Régions AWS

Le mode d'isolation des locataires est pris en charge dans toutes les régions commerciales, à l'exception de l'Asie-Pacifique (Nouvelle Zélande).

Considérations

Lorsque vous utilisez l'isolation des locataires avec vos fonctions d'événement Lambda, gardez à l'esprit les points suivants :

- Configuration immuable : l'isolation des locataires est une propriété de fonction immuable. Elle ne peut être activée que lors de la création d'une fonction.
- Paramètre tenant-id requis : les fonctions événementielles utilisant le mode d'isolation des locataires doivent être invoquées avec un `tenant-id` paramètre. L'omission de ce paramètre entraîne l'échec des appels de fonctions.
- Le rôle d'exécution s'applique à tous les locataires : les invocations provenant de tous les locataires utilisent les autorisations définies dans le rôle d'exécution de votre fonction d'événement Lambda.
- Concurrence : aucun changement n'est apporté au comportement simultané ou à la mise à l'échelle de votre fonction événementielle lorsque vous utilisez l'isolation des locataires. Lambda impose une limite de 2 500 environnements d'exécution isolés par les locataires (actifs ou inactifs) pour 1 000 exécutions simultanées configurées pour votre fonction d'événement Lambda.

Tarification

Vous êtes débité lorsque Lambda crée un nouvel environnement d'exécution isolé par les locataires. Le prix dépend de la quantité de mémoire que vous allouez à votre fonction événementielle et de l'architecture du processeur que vous utilisez. Pour en savoir plus, consultez Pricing AWS Lambda (Tarification).

Mode d'isolation

Le tableau suivant décrit les différences entre les fonctions d'événement Lambda avec et sans isolation des locataires.

Fonctionnalité	Avec isolation des locataires	Sans isolement des locataires
Type d'isolation	Tenant-level isolation	Function-level isolation
Réutilisation de l'environnement	Les environnements d'exécution ne sont jamais réutilisés entre différents locataires	Les environnements d'exécution peuvent être réutilisés lors des invocations de la même fonction
Isolation des données	Les données des autres locataires ne sont pas accessibles	Les données des appels précédents de la même version de fonction peuvent être accessibles
Démarrages à froid	Davantage de démarrages à froid en raison des environnements spécifiques aux locataires	Moins de démarrages à froid grâce à la réutilisation dans l'environnement
Tarification	Frais supplémentaires en plus de la tarification Lambda standard	Tarification Lambda standard

Activation de l'isolation des locataires pour les fonctions d'événement Lambda

Pour activer le mode d'isolation des locataires, créez une nouvelle fonction d'événement Lambda. Vous ne pouvez pas activer l'isolation des locataires sur les fonctions d'événement existantes.

Rubriques

- Activation de l'isolation des locataires (console)
- Permettre l'isolement des locataires (AWS CLI)
- Activation de l'isolation des locataires (API)
- Permettre l'isolement des locataires (CloudFormation)

Activation de l'isolation des locataires (console)

Pour créer une fonction d'événement Lambda à l'aide de la console

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez Create Event Function.
3. Sélectionnez Créer à partir de zéro.
4. Dans le volet Informations de base, pour Nom de la fonction, saisissez **`image-analysis`**.
5. Pour Runtime, choisissez l'un des environnements d'exécution Lambda pris en charge.
6. Sous Configurations supplémentaires, mode d'isolation des locataires, sélectionnez Activer.
7. Vérifiez vos paramètres, puis choisissez Create Event Function.

Permettre l'isolement des locataires (AWS CLI)

Création d'une fonction événementielle avec isolation des locataires

Lorsque vous créez une nouvelle fonction d'événement à l'aide de la CLI, ajoutez l'`--tenancy-config '{"TenantIsolationMode": "PER_TENANT"}'` option à votre demande de création de fonction. Exemple :

```
aws lambda create-function \
    --function-name image-analysis \
    --runtime nodejs24.x \
    --zip-file fileb://image-analysis-function.zip \
```

```
    --handler image-analysis-function.handler \
    --role arn:aws:iam:123456789012:role/execution-role \
    --tenancy-config '{"TenantIsolationMode": "PER_TENANT"}'
```

Activation de l'isolation des locataires (API)

Pour activer l'isolation des locataires à l'aide de l'API Lambda

1. Créez une nouvelle fonction d'événement avec l'isolation des locataires activée en utilisant l'action CreateFunctionAPI avec le `TenancyConfig` paramètre.
2. Vérifiez que l'isolation des locataires est activée pour la fonction d'événement en utilisant l'GetFunctionConfigurationaction. Si la réponse indique que `TenantIsolationMode` c'est le cas`PER_TENANT`, l'isolation des locataires est activée pour la fonction d'événement :

   ```
   "TenancyConfig": {
           "TenantIsolationMode": "PER_TENANT"
       }
   ```

Invoquez la version de la fonction avec l'action Invoke. Pour plus d'informations, consultez Invocation de fonctions d'événement Lambda avec isolation des locataires.

Permettre l'isolement des locataires (CloudFormation)

Le CloudFormation modèle suivant crée une nouvelle fonction d'événement Lambda avec l'isolation des locataires activée :

```
MyLambdaFunction:
    Type: AWS::Lambda::Function
    Properties:
      FunctionName: my-sample-python-lambda
      Runtime: python3.14
      Role: !GetAtt LambdaExecutionRole.Arn
      Handler: index.lambda_handler
      TenancyConfig:
        TenantIsolationMode: PER_TENANT
      Code:
        ZipFile: |
          import json

          def lambda_handler(event, context):
```

```
            return {
                'statusCode': 200,
                'body': json.dumps(f'Hello from Lambda! Tenant-ID:
{context.tenant_id}')
            }
    Timeout: 10
    MemorySize: 128
```

Invocation de fonctions d'événement Lambda avec isolation des locataires

Lorsque vous appelez une fonction d'événement pour laquelle l'isolation des locataires est activée, vous devez fournir un `tenant-id` paramètre. Ce paramètre garantit que votre appel de fonction d'événement est traité dans un environnement d'exécution dédié à ce locataire spécifique.

Invocation de fonctions événementielles avec isolation des locataires (AWS CLI)

Invocation synchrone

Pour les appels synchrones, ajoutez le `--tenant-id` paramètre à votre commande Invoke :

```
aws lambda invoke \
    --function-name image-analysis \
    --tenant-id blue \
    response.json
```

invocation asynchrone

Pour les appels asynchrones, incluez à la fois les paramètres et : `--tenant-id --invocation-type Event`

```
aws lambda invoke \
    --function-name image-analysis \
    --tenant-id blue \
    --invocation-type Event \
    response.json
```

Invocation de fonctions d'événement avec isolation des locataires (API)

Lorsque vous utilisez directement l'action d'API Invoke, incluez l'identifiant du locataire à l'aide du `X-Amzn-Tenant-Id` paramètre dans votre demande.

Exemple de demande d'API

```
POST /2015-03-31/functions/image-analysis/invocations HTTP/1.1
Host: lambda.us-east-1.amazonaws.com
Content-Type: application/json
Authorization: AWS4-HMAC-SHA256 Credential=...
X-Amz-Tenant-Id: blue
```

```
{
    "key1": "value1",
    "key2": "value2"
}
```

Invocation de fonctions événementielles avec isolation des locataires (API Gateway)

Lorsque vous utilisez les API REST d'API Gateway pour déclencher des fonctions d'événement Lambda isolées par les locataires, vous devez configurer API Gateway pour mapper les propriétés des demandes du client à l'en-tête `X-Amz-Tenant-Id` attendu par Lambda. API Gateway utilise l'action d'API Invoke de Lambda, qui nécessite que l'ID du locataire soit transmis à l'aide de l'en-tête `X-Amz-Tenant-Id` HTTP. Vous pouvez configurer API Gateway pour injecter cet en-tête HTTP dans la demande d'appel Lambda avec une valeur obtenue à partir des propriétés de demande du client telles que les en-têtes HTTP, les paramètres de requête ou les paramètres de chemin. Vous devez d'abord mapper la propriété de la demande du client avant de pouvoir remplacer l'`X-Amz-Tenant-Id`en-tête.

> **Note**
>
> Vous ne pouvez pas utiliser les API HTTP pour appeler des fonctions d'événement Lambda isolées par les locataires, car il n'est pas possible de remplacer l'en-tête. `X-Amz-Tenant-Id`

Utilisation des en-têtes de demande

Configurez votre intégration API Gateway pour mapper un en-tête personnalisé entre la demande du client et l'`X-Amz-Tenant-Id`en-tête. L'exemple suivant montre une demande client avec un `x-tenant-id` en-tête :

```
POST /api/process HTTP/1.1
Host: your-api-id.execute-api.us-east-1.amazonaws.com
Content-Type: application/json
x-tenant-id: blue

{
    "data": "sample payload"
}
```

Dans la configuration de votre méthode API Gateway, vous devez :

1. Activez le paramètre d'en-tête de demande du client (par exemple,`method.request.header.x-tenant-id`)
2. Mappez l'en-tête du client à l'en-tête d'intégration Lambda en utilisant `integration.request.header.X-Amz-Tenant-Id`

Utilisation des paramètres de requête

De même, vous pouvez associer les paramètres de requête à l'`X-Amz-Tenant-Id`en-tête :

```
GET /api/process?tenant-id=blue&data=sample HTTP/1.1
Host: your-api-id.execute-api.us-east-1.amazonaws.com
```

Configurez la méthode pour activer le paramètre de requête et mappez-le à l'en-tête d'intégration.

Invocation de fonctions d'événement avec isolation des locataires (SDK)

Lorsque vous utilisez AWS des SDK pour invoquer des fonctions d'événement isolées par le locataire, incluez l'identifiant du locataire dans votre demande d'invocation.

Python

```
import boto3
import json

lambda_client = boto3.client('lambda')

response = lambda_client.invoke(
    FunctionName='image-analysis',
    TenantId='blue',
    Payload=json.dumps({
        'key1': 'value1',
        'key2': 'value2'
    })
)

result = json.loads(response['Payload'].read())
```

Node.js

```
const AWS = require('aws-sdk');
```

```
const lambda = new AWS.Lambda();

const params = {
    FunctionName: 'image-analysis',
    TenantId: 'blue',
    Payload: JSON.stringify({
        key1: 'value1',
        key2: 'value2'
    })
};

lambda.invoke(params, (err, data) => {
    if (err) {
        console.error(err);
    } else {
        const result = JSON.parse(data.Payload);
        console.log(result);
    }
});
```

Java

```
import software.amazon.awssdk.services.lambda.LambdaClient;
import software.amazon.awssdk.services.lambda.model.InvokeRequest;
import software.amazon.awssdk.services.lambda.model.InvokeResponse;
import software.amazon.awssdk.core.SdkBytes;

public class TenantIsolationExample {

    public static void main(String[] args) {
        LambdaClient lambdaClient = LambdaClient.create();

        String payload = "{\"key1\": \"value1\", \"key2\": \"value2\"}";

        InvokeRequest request = InvokeRequest.builder()
                .functionName("image-analysis")
                .tenantId("blue")
                .payload(SdkBytes.fromUtf8String(payload))
                .build();

        InvokeResponse response = lambdaClient.invoke(request);
    }
}
```

Accès à l'identifiant du locataire dans le code Lambda Event Function

Lorsque l'isolation des locataires est activée dans votre fonction d'événement Lambda, l'identifiant de locataire utilisé pour appeler votre fonction d'événement est mis à disposition dans l'objet de contexte transmis à votre gestionnaire de fonctions d'événement. Vous pouvez utiliser cet identifiant pour implémenter des fonctionnalités de logique, de surveillance et de débogage spécifiques au locataire.

Rubriques

- Accès à l'identifiant du locataire
- Modèles d'utilisation courants
- Surveillance et débogage

Accès à l'identifiant du locataire

L'identifiant du locataire est disponible via la `tenantId` propriété de l'objet de contexte. Notez que cette propriété est disponible pendant la phase d'appel, et non pendant la phase d'initialisation.

Python

```
def lambda_handler(event, context):
    tenant_id = context.tenant_id
    print(f"Processing request for tenant: {tenant_id}")

    # Implement tenant-specific logic
    if tenant_id == "blue":
        return process_blue_tenant(event)
    elif tenant_id == "green":
        return process_green_tenant(event)
    else:
        return process_default_tenant(event)
```

Node.js

```
exports.handler = async (event, context) => {
    const tenantId = context.tenantId;
    console.log(`Processing request for tenant: ${tenantId}`);

    // Implement tenant-specific logic
    switch (tenantId) {
        case 'blue':
```

```
            return processBlueTenant(event);
        case 'green':
            return processGreenTenant(event);
        default:
            return processDefaultTenant(event);
    }
};
```

Java

```
public class TenantHandler implements RequestHandler<Map<String, Object>, String> {

    @Override
    public String handleRequest(Map<String, Object> event, Context context) {
        String tenantId = context.getTenantId();
        System.out.println("Processing request for tenant: " + tenantId);

        // Implement tenant-specific logic
        switch (tenantId) {
            case "blue":
                return processBlueTenant(event);
            case "green":
                return processGreenTenant(event);
            default:
                return processDefaultTenant(event);
        }
    }
}
```

Modèles d'utilisation courants

Voici les méthodes les plus courantes pour utiliser l'identifiant du locataire dans le code de votre fonction d'événement :

Tenant-specific configuration

Utilisez l'ID du locataire pour charger la configuration ou les paramètres spécifiques au locataire :

```
def lambda_handler(event, context):
    tenant_id = context.tenant_id

    # Load tenant-specific configuration
```

```
    config = load_tenant_config(tenant_id)
    database_url = config['database_url']
    api_key = config['api_key']

    # Process with tenant-specific settings
    return process_request(event, database_url, api_key)
```

Tenant-specific accès aux données

Utilisez l'ID du locataire pour garantir l'isolation des données et le contrôle d'accès :

```
import boto3

def lambda_handler(event, context):
    tenant_id = context.tenant_id

    # Ensure data access is scoped to the tenant
    dynamodb = boto3.resource('dynamodb')
    table = dynamodb.Table('user_data')

    user_id = event.get('userId')

    response = table.get_item(
        Key={
            'tenant_id': tenant_id,
            'user_id': user_id
        }
    )

    return process_results(response.get('Item'), tenant_id)
```

Surveillance et débogage

L'identifiant du locataire est automatiquement inclus dans les journaux Lambda lorsque la journalisation JSON est activée, ce qui facilite le suivi et le débogage des problèmes spécifiques au locataire. Vous pouvez également utiliser l'ID du locataire pour des mesures et un suivi personnalisés.

Example Métriques personnalisées avec identifiant de locataire

L'exemple suivant montre comment utiliser l'ID du locataire pour créer des CloudWatch métriques spécifiques au locataire afin de surveiller les modèles d'utilisation et les performances par locataire :

```
import boto3

def lambda_handler(event, context):
    tenant_id = context.tenant_id
    cloudwatch = boto3.client('cloudwatch')

    # Record tenant-specific metrics
    cloudwatch.put_metric_data(
        Namespace='MyApp/TenantMetrics',
        MetricData=[
            {
                'MetricName': 'RequestCount',
                'Dimensions': [
                    {
                        'Name': 'TenantId',
                        'Value': tenant_id
                    }
                ],
                'Value': 1,
                'Unit': 'Count'
            }
        ]
    )

    return process_request(event, tenant_id)
```

Surveillance des fonctions d'événement Lambda avec isolation des locataires

Vous pouvez surveiller vos fonctions Lambda isolées par vos locataires à l'aide d'Amazon CloudWatch et en accédant aux données de télémétrie en temps réel pour les extensions à l'aide de l'API de télémétrie. AWS X-Ray

Comprendre la journalisation en mode isolé pour les locataires

Pour les fonctions utilisant l'isolation des locataires, Lambda inclut automatiquement l'identifiant du locataire dans les journaux des fonctions lorsque la journalisation JSON est activée, ce qui facilite le suivi et le débogage des problèmes spécifiques aux locataires. Lambda crée un flux de CloudWatch journal distinct pour chaque environnement d'exécution. Vous pouvez utiliser CloudWatch Logs Insights pour rechercher les flux de journaux appartenant à un locataire en particulier en filtrant par identifiant de locataire :

```
fields @logStream, @message
| filter tenantId=='BlueTenant' or record.tenantId=='BlueTenant'
| stats count() as logCount by @logStream
| sort @timestamp desc
```

Vous pouvez également utiliser ce paramètre pour récupérer les journaux spécifiques au locataire dans tous les flux de journaux :

```
fields @message
| filter tenantId=='BlueTenant' or record.tenantId=='BlueTenant'
| limit 1000
```

La `tenantId` propriété est incluse pour les événements des plateformes (tels que `platform.start` et`platform.report`) et les journaux personnalisés que vous imprimez dans votre code de fonction, comme indiqué ci-dessous :

```
{
    "time": "2025-10-13T19:48:06.990Z",
    "type": "platform.start",
    "record": {
        "requestId": "a0f40320-b43c-44b3-91bf-d5b5240a1bed",
        "functionArn": "arn:aws:lambda:us-east-1:xxxxxx:function:multitenant-
function-1",
```

```
        "version": "$LATEST",
        "tenantId": "BlueTenant""
    }
}
{
    "timestamp": "2025-10-13T19:48:06.992Z",
    "level": "INFO",
    "requestId": "a0f40320-b43c-44b3-91bf-d5b5240a1bed",
    "tenantId": "BlueTenant"",
    "message": "custom log line1"
}
{
    "timestamp": "2025-10-13T19:48:07.022Z",
    "level": "WARN",
    "requestId": "a0f40320-b43c-44b3-91bf-d5b5240a1bed",
    "tenantId": "BlueTenant"",
    "message": "custom log line2"
}
```

Résolution des problèmes d'isolation des locataires pour les fonctions d'événement Lambda

Cette page aborde les problèmes courants qui se produisent lors de l'utilisation de l'isolation des locataires pour AWS Lambda.

InvalidParameterValueException

Erreur : la configuration de l'ID du locataire n'est pas spécifiée ou n'est pas transmise à une fonction lorsque l'isolation du locataire n'est pas activée.

Causes courantes

Cette erreur se produit lors de l'appel d'une fonction isolée par le locataire sans identifiant de locataire, ou lors de l'appel d'une fonction non isolée par le locataire avec un identifiant de locataire.

Résolution

Ajoutez un ID de locataire si l'isolation des locataires est activée dans la fonction, ou supprimez l'ID de locataire si l'isolation des locataires n'est pas activée dans la fonction.

TooManyRequestsException

Erreur : taux dépassé

Causes courantes

Outre la limitation du débit basée sur le nombre maximal d'exécutions simultanées et le taux de dimensionnement des fonctions, Lambda limite le nombre maximum d'environnements d'exécution sensibles aux locataires (actifs ou inactifs) pouvant exister à la fois à 2 500 pour 1 000 exécutions simultanées de votre fonction.

Résolution

Pour résoudre ce problème, vous pouvez soit réduire la fréquence à laquelle les demandes d'invocation avec des identifiants de locataire uniques sont effectuées, soit implémenter des nouvelles tentatives avec backoff et jitter, soit demander une augmentation de la limite de simultanéité des fonctions.

Instances gérées par Lambda

Avec les instances gérées Lambda, vous pouvez exécuter des fonctions événementielles Lambda sur vos instances Amazon EC2 de génération actuelle, y compris Graviton4, des instances optimisées pour le réseau et d'autres options de calcul spécialisées. Vous n'avez pas besoin de gérer les cycles de vie des instances, l'application de correctifs, le routage, l'équilibrage de charge ou les politiques de dimensionnement du système d'exploitation et du langage d'exécution. Avec les instances gérées Lambda, vous bénéficiez des avantages tarifaires d'EC2, notamment des plans d'épargne EC2 et des instances réservées. Les instances gérées Lambda ne prennent actuellement en charge que les fonctions événementielles Lambda.

Pour obtenir la liste des types d'instances pris en charge, consultez le AWS Lambda Tarification page et sélectionnez votre Région AWS.

Fonctionnalités clés

Les instances gérées Lambda fournissent les fonctionnalités suivantes :

- Choisissez les instances appropriées - Sélectionnez instances appropriées en fonction des exigences de performances et de coûts, y compris l'accès aux processeurs les plus récents tels que Graviton4, des ratios mémoire-processeur configurables et une mise en réseau à bande passante élevée.
- Approvisionnement automatique - AWS provisionne automatiquement les instances appropriées et fait tourner les environnements d'exécution des fonctions.
- Mise à l'échelle dynamique - Les instances évoluent de manière dynamique en fonction des modèles de trafic de vos fonctions.
- Expérience entièrement gérée - AWS gère la gestion de l'infrastructure, la mise à l'échelle, l'application de correctifs et le routage, avec les mêmes intégrations complètes de sources d'événements que vous connaissez bien.

Quand utiliser les instances gérées Lambda

Envisagez les instances gérées Lambda pour les cas d'utilisation suivants :

- Charges de travail prévisibles à volume élevé - Idéal pour les charges de travail stables sans pics de trafic inattendus. Les instances gérées Lambda s'adaptent pour gérer le doublement du trafic en cinq minutes par défaut.

- Performance-critical applications - Accès aux processeurs les plus récents, à des ratios mémoire-processeur variables et à un débit réseau élevé
- Exigences réglementaires - Besoins de gouvernance granulaire avec contrôle du VPC et du placement des instances
- Une variété d'applications - Event-driven applications, media/data traitement, applications Web et charges de travail existantes migrant vers une solution sans serveur

Comment ça marche

Les instances gérées Lambda utilisent des fournisseurs de capacité comme base pour exécuter vos fonctions :

1. Création d'un fournisseur de capacités - Définissez l'endroit où vos fonctions s'exécutent en spécifiant la configuration du VPC et, éventuellement, les exigences en matière d'instance et la configuration de dimensionnement
2. Créez votre fonction - Créez des fonctions Lambda comme d'habitude et associez-les à un fournisseur de capacité
3. Publier une version de fonction - Les versions des fonctions deviennent actives sur les instances des fournisseurs de capacité une fois publiées

Lorsque vous publiez une version de fonction avec un fournisseur de capacité, Lambda lance des instances gérées dans votre compte. Il lance trois instances par défaut pour la résilience AZ et démarre trois environnements d'exécution avant de marquer la version de votre fonction comme ACTIVE. Si vous attachez une fonction à un fournisseur de capacité existant qui exécute déjà d'autres fonctions, Lambda risque de ne pas créer de nouvelles instances si les instances disponibles disposent déjà de la capacité nécessaire pour s'adapter aux environnements d'exécution de la nouvelle fonction.

Modèle de simultanéité

Les instances gérées Lambda prennent en charge les appels multisimultanés, dans lesquels un environnement d'exécution peut gérer plusieurs appels en même temps. Cela diffère du type de calcul Lambda (par défaut), qui fournit un modèle de simultanéité unique dans lequel un environnement d'exécution peut exécuter un maximum d'une invocation à la fois. Multi-concurrency permet une meilleure utilisation de vos instances EC2 sous-jacentes et est particulièrement bénéfique pour IO-heavy applications telles que les services Web ou les tâches par lots. Cette modification du

modèle d'exécution signifie que la sécurité des threads, la gestion de l'état et l'isolation du contexte doivent être gérées différemment selon le runtime.

Location et isolement

Le type de calcul Lambda (par défaut) est mutualisé et utilise la technologie Firecracker MicroVM pour isoler les environnements d'exécution exécutés sur des flottes Lambda partagées. Les instances gérées Lambda s'exécutent sur votre compte et fournissent le matériel EC2 le plus récent et les dernières options tarifaires. Les instances gérées utilisent des conteneurs exécutés sur des instances EC2 Nitro pour assurer l'isolation plutôt que Firecracker. Les fournisseurs de capacité constituent la limite de sécurité pour les fonctions Lambda. Les fonctions s'exécutent dans des conteneurs au sein d'instances.

Comprendre les instances gérées

Les fonctions Lambda Managed Instances s'exécutent sur Instances gérées EC2 dans votre compte. Ces instances sont entièrement gérées par Lambda, ce qui signifie que vous disposez d'autorisations limitées sur celles-ci par rapport aux instances EC2 standard. Vous pouvez identifier les instances gérées Lambda dans votre compte en :

- La présence de `Operator` champ dans EC2 `DescribeInstances` sortie
- Le `aws:lambda:capacity-provider` tag sur l'instance

Vous ne pouvez pas effectuer d'opérations EC2 standard directement sur ces instances, comme les arrêter manuellement. Pour détruire les instances gérées, supprimez le fournisseur de capacité associé. Lambda met ensuite fin aux instances dans le cadre du processus de suppression du fournisseur de capacité.

Les instances gérées sont masquées par défaut dans les vues de votre console EC2 et dans les opérations de liste d'API. Vous pouvez régler la visibilité à l'aide du paramètre de visibilité des ressources gérées. Les instances gérées restent pleinement opérationnelles et facturables dans votre AWS compte.

Tarification

Utilisations des instances gérées Lambda EC2-based tarification avec des frais de gestion de 15 % en plus du coût de l'instance EC2. Ce modèle tarifaire prend en charge les plans d'épargne EC2, les instances réservées et toute autre remise tarifaire appliquée à votre utilisation d'EC2. Consultez la page de tarification pour plus de détails : https://aws.amazon.com/lambda/pricing/

Pour comparer le coût de l'exécution de vos fonctions sur Lambda default, les instances gérées Lambda et Amazon EC2 autogéré, utilisez Calculateur de tarification des instances gérées Lambda.

Important : Les remises tarifaires EC2 s'appliquent uniquement au calcul EC2 sous-jacent, et non aux frais de gestion.

Différences entre les instances gérées Lambda et le type de calcul Lambda (par défaut)

Les instances gérées Lambda modifient la façon dont Lambda traite les demandes par rapport à Lambda (par défaut).

Principales différences :

	Lambda (par défaut)	Instances gérées par Lambda
Modèle de concurrence	Modèle de simultanéité unique dans lequel un environnement d'exécution peut prendre en charge un maximum d'une invocation à la fois	Multi-concurrent invocations dans lesquelles un environnement d'exécution peut gérer plusieurs invocations simultanément, augmentant ainsi le débit, en particulier pour IO-heavy applications
Location et isolement	Multi-tenant, utilisant la technologie Firecracker MicroVM pour isoler les environnements d'exécution exécutés sur des flottes Lambda partagées	Exécutez-le dans votre compte en utilisant EC2 Nitro pour assurer l'isolation. Les fournisseurs de capacité constituent la limite de sécurité, les fonctions s'exécutant dans des conteneurs au sein des instances
Modèle de tarification	Per-request tarification de la durée	Instance-based tarification avec les modèles de tarification EC2, y compris On-Demand et des instances réservées, ainsi que des options d'économie telles que Compute Savings Plans

	Lambda (par défaut)	Instances gérées par Lambda
Comportement de mise à l'échelle	Évolue lorsqu'il n'existe pas d'environnement d'exécution libre pour gérer une invocation entrante (démarrage à froid). Passe à zéro sans trafic	Évolue de manière asynchron e en fonction de l'utilisation des ressources du processeur uniquement, sans démarrage à froid. S'adapte à des environne ments d'exécution minimaux configurés sans trafic
Idéal pour	Fonctions soumises à un trafic en rafale pouvant supporter un certain temps de démarrage à froid, ou applications sans charge soutenue qui bénéficient d'une évolutivité à zéro	Le trafic prévisible à volume élevé fonctionne lorsque vous souhaitez bénéficier de la flexibilité, des plans tarifaires et des options matérielles d'EC2

Étapes suivantes

- En savoir plus sur concepts de base pour les instances gérées Lambda
- Démarrez avec les instances gérées Lambda
- En savoir plus sur fournisseurs de capacité pour les instances gérées Lambda
- Comprenez mise à l'échelle pour les instances gérées Lambda
- En savoir plus sur déploiement et mise à jour des fonctions des instances gérées Lambda
- Révision temps d'exécution pris en charge
- Consultez les guides spécifiques à l'exécution pour Java, Node.js, et Python
- Configurez Connectivité VPC pour vos fournisseurs de capacité
- Comprenez sécurité et autorisations pour les instances gérées Lambda
- Révision quotas et limites
- Résoudre les problèmes liés aux instances gérées Lambda

Commencer à utiliser les instances gérées Lambda

Création d'une fonction d'instance gérée Lambda (console)

Vous pouvez utiliser la console Lambda pour créer une fonction d'instance gérée qui s'exécute sur des instances Amazon EC2 gérées par un fournisseur de capacité.

Important : Avant de créer une fonction d'instance gérée, vous devez d'abord créer un fournisseur de capacité. Ces fonctions d'événement Lambda nécessitent un fournisseur de capacité pour définir l'infrastructure Amazon EC2 qui exécute vos fonctions.

Pour créer une fonction d'instance gérée Lambda (console)

1. Ouvrez la console Lambda.
2. Choisissez Capacity providers dans le volet de navigation de gauche.
3. Choisissez Créer un fournisseur de capacité.
4. Dans la section Paramètres du fournisseur de capacité, entrez le nom de votre fournisseur de capacité.
5. Sélectionnez le VPC et les autorisations pour votre fournisseur de capacité. Vous pouvez soit en utiliser un existant, soit en créer un nouveau. Pour plus d'informations sur la création du rôle d'opérateur requis, voir Rôle d'opérateur Lambda pour les instances gérées Lambda.
6. Développez Advanced settings (Paramètres avancés).
7. Définissez les exigences de votre instance en choisissant l'architecture du processeur et les types d'instance.
8. Sous Mise à l'échelle automatique, spécifiez le nombre maximum de vCPU EC2 pour votre fournisseur de capacité. Vous pouvez également choisir le mode de dimensionnement manuel de l'instance pour définir votre propre valeur de mise à l'échelle pour un contrôle précis.
9. Choisissez Créer un fournisseur de capacité pour en créer un nouveau.
10. Choisissez ensuite Create function.
11. Sélectionnez Créer à partir de zéro.
12. Dans le volet Informations de base, indiquez le nom de la fonction.
13. Pour Runtime, choisissez l'un des Runtimes pris en charge.
14. Choisissez l'architecture de votre fonction (identique à celle que vous avez sélectionnée pour le fournisseur de capacité). Par défaut, x86_64.

15. Sous Autorisations, assurez-vous d'avoir l'autorisation pour le rôle d'exécution choisi. Sinon, vous pouvez créer un nouveau rôle.
16. Sous Configurations supplémentaires, sélectionnez le type de calcul en tant qu'instances gérées Lambda.
17. L'ARN du fournisseur de capacité que vous avez créé au cours des étapes précédentes doit être présélectionné.
18. Choisissez la taille de la mémoire et le ratio de mémoire de l'environnement d'exécution (GiB) par vCPU.
19. Choisissez Créer une fonction.

Votre fonction d'instance gérée Lambda est créée et fournit de la capacité au fournisseur de capacité que vous avez spécifié. La création d'une fonction prend généralement plusieurs minutes. Une fois terminé, vous pouvez modifier le code de votre fonction et exécuter votre premier test.

Création d'une fonction d'instance gérée Lambda (AWS CLI)

Conditions préalables

Avant de commencer, assurez-vous de disposer des éléments suivants :

- AWS CLI — Installez et configurez la AWS CLI. Pour plus d'informations, voir Installation ou mise à jour de la dernière version de la AWS CLI.
- Autorisations IAM : votre utilisateur ou rôle IAM doit être autorisé à créer des fonctions Lambda, à fournir des capacités et à transmettre des rôles IAM. Notez que vous en aurez également besoin `iam:CreateServiceLinkedRole` si c'est la première fois que vous créez un fournisseur de capacité dans le compte ou si le rôle lié au service (SLR) a été supprimé.

Étape 1 : créer les rôles IAM requis

Les instances gérées Lambda nécessitent deux rôles IAM : un rôle d'exécution pour votre fonction et un rôle d'opérateur pour le fournisseur de capacité. Le rôle d'opérateur permet à Lambda de lancer, de résilier et de surveiller les instances Amazon EC2 en votre nom. Le rôle d'exécution de la fonction accorde à la fonction l'autorisation d'accéder à d'autres AWS services et ressources.

Pour créer le rôle d'exécution Lambda

1. Créez un document de politique de confiance qui permet à Lambda d'assumer le rôle :

```
cat > lambda-trust-policy.json << 'EOF'
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
EOF
```

2. Créez le rôle d'exécution :

```
aws iam create-role \
  --role-name MyLambdaExecutionRole \
  --assume-role-policy-document file://lambda-trust-policy.json
```

3. Joignez la politique d'exécution de base :

```
aws iam attach-role-policy \
  --role-name MyLambdaExecutionRole \
  --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole
```

Pour créer le rôle d'opérateur fournisseur de capacité

1. Créez un document de politique de confiance qui permet à Lambda d'assumer le rôle d'opérateur :

```
cat > operator-trust-policy.json << 'EOF'
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
```

```
    }
  ]
}
EOF
```

2. Créez le rôle d'opérateur :

```
aws iam create-role \
  --role-name MyCapacityProviderOperatorRole \
  --assume-role-policy-document file://operator-trust-policy.json
```

3. Joignez la politique d'autorisation EC2 requise :

```
aws iam attach-role-policy \
  --role-name MyCapacityProviderOperatorRole \
  --policy-arn arn:aws:iam::aws:policy/AWSLambdaManagedEC2ResourceOperator
```

Étape 2 : configurer les ressources VPC

Les instances gérées Lambda s'exécutent dans votre VPC et nécessitent un sous-réseau et un groupe de sécurité.

Pour créer des ressources VPC

1. Créez un VPC :

```
VPC_ID=$(aws ec2 create-vpc \
  --cidr-block 10.0.0.0/16 \
  --query 'Vpc.VpcId' \
  --output text)
```

2. Créez un sous-réseau :

```
SUBNET_ID=$(aws ec2 create-subnet \
  --vpc-id $VPC_ID \
  --cidr-block 10.0.1.0/24 \
  --query 'Subnet.SubnetId' \
  --output text)
```

3. Créez un groupe de sécurité :

```
SECURITY_GROUP_ID=$(aws ec2 create-security-group \
```

```
  --group-name my-capacity-provider-sg \
  --description "Security group for Lambda Managed Instances" \
  --vpc-id $VPC_ID \
  --query 'GroupId' \
  --output text)
```

Remarque : Les fonctions de vos instances gérées Lambda nécessitent une configuration VPC pour accéder à des ressources extérieures au VPC et pour transmettre des données de télémétrie à Logs and. CloudWatch X-Ray Pour plus de détails sur la configuration, consultez la section Mise en réseau pour les instances gérées Lambda.

Étape 3 : Créer un fournisseur de capacité

Un fournisseur de capacité gère les instances EC2 qui exécutent vos fonctions Lambda.

Pour créer un fournisseur de capacité

```
ACCOUNT_ID=$(aws sts get-caller-identity --query Account --output text)

aws lambda create-capacity-provider \
  --capacity-provider-name my-capacity-provider \
  --vpc-config SubnetIds=[$SUBNET_ID],SecurityGroupIds=[$SECURITY_GROUP_ID] \
  --permissions-config CapacityProviderOperatorRoleArn=arn:aws:iam::${ACCOUNT_ID}:role/
MyCapacityProviderOperatorRole \
  --instance-requirements Architectures=[x86_64] \
  --capacity-provider-scaling-config MaxVCpuCount=30
```

Cette commande crée un fournisseur de capacité avec la configuration suivante :

- Configuration VPC — Spécifie le sous-réseau et le groupe de sécurité pour les instances EC2
- Autorisations — Définit le rôle IAM que Lambda utilise pour gérer les instances EC2
- Exigences relatives à l'instance — Spécifie l'architecture x86_64
- Configuration évolutive : définit un maximum de 30 vCPU pour le fournisseur de capacité

Étape 4 : Création d'une fonction Lambda avec du code en ligne

Pour créer une fonction avec du code en ligne

1. Tout d'abord, créez une fonction Python simple et empaquez-la en ligne :

```
# Create a temporary directory for the function code
mkdir -p /tmp/my-lambda-function
cd /tmp/my-lambda-function

# Create a simple Python handler
cat > lambda_function.py << 'EOF'
import json

def lambda_handler(event, context):
    return {
        'statusCode': 200,
        'body': json.dumps({
            'message': 'Hello from Lambda Managed Instances!',
            'event': event
        })
    }
EOF

# Create a ZIP file
zip function.zip lambda_function.py
```

2. Créez la fonction Lambda à l'aide du fichier ZIP intégré :

```
ACCOUNT_ID=$(aws sts get-caller-identity --query Account --output text)
REGION=$(aws configure get region)

aws lambda create-function \
  --function-name my-managed-instance-function \
  --package-type Zip \
  --runtime python3.13 \
  --handler lambda_function.lambda_handler \
  --zip-file fileb:///tmp/my-lambda-function/function.zip \
  --role arn:aws:iam::${ACCOUNT_ID}:role/MyLambdaExecutionRole \
  --architectures x86_64 \
  --memory-size 2048 \
  --ephemeral-storage Size=512 \
  --capacity-provider-config
 LambdaManagedInstancesCapacityProviderConfig={CapacityProviderArn=arn:aws:lambda:
${REGION}:${ACCOUNT_ID}:capacity-provider:my-capacity-provider}
```

La fonction est créée avec :

- Runtime — Python 3.13
- Handler — La `lambda_handler` fonction dans `lambda_function.py`
- Mémoire — 2048 Mo
- Stockage éphémère — 512 Mo
- Fournisseur de capacité : liens vers le fournisseur de capacité que vous avez créé

Étape 5 : Publier une version de fonction

Pour exécuter votre fonction sur des instances gérées Lambda, vous devez publier une version.

Pour publier une version de fonction

```
aws lambda publish-version \
  --function-name my-managed-instance-function
```

Cette commande publie la version 1 de votre fonction et la déploie auprès du fournisseur de capacité.

Étape 6 : Invoquez votre fonction

Après la publication, vous pouvez appeler votre fonction.

Pour appeler votre fonction

```
aws lambda invoke \
  --function-name my-managed-instance-function:1 \
  --payload '{"name": "World"}' \
  response.json

# View the response
cat response.json
```

La fonction s'exécute sur les instances EC2 gérées par votre fournisseur de capacité et renvoie une réponse.

Nettoyage

Pour éviter d'encourir des frais, supprimez les ressources que vous avez créées :

1. Supprimez la fonction :

```
aws lambda delete-function --function-name my-managed-instance-function
```

2. Supprimez le fournisseur de capacité :

```
aws lambda delete-capacity-provider --capacity-provider-name my-capacity-provider
```

3. Supprimez les ressources VPC :

```
aws ec2 delete-security-group --group-id $SECURITY_GROUP_ID
aws ec2 delete-subnet --subnet-id $SUBNET_ID
aws ec2 delete-vpc --vpc-id $VPC_ID
```

4. Supprimez les rôles IAM :

```
aws iam detach-role-policy \
  --role-name MyLambdaExecutionRole \
  --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole
aws iam detach-role-policy \
  --role-name MyCapacityProviderOperatorRole \
  --policy-arn arn:aws:iam::aws:policy/AWSLambdaManagedEC2ResourceOperator

aws iam delete-role --role-name MyLambdaExecutionRole
aws iam delete-role --role-name MyCapacityProviderOperatorRole
```

Concepts de base

Les instances gérées Lambda présentent plusieurs concepts fondamentaux qui diffèrent des fonctions Lambda traditionnelles. Il est essentiel de comprendre ces concepts pour déployer et gérer efficacement vos fonctions Lambda Event sur l'infrastructure EC2.

Fournisseurs de capacités constituent la base des instances gérées Lambda. Un fournisseur de capacité définit l'infrastructure informatique sur laquelle vos fonctions s'exécutent, y compris la configuration du VPC, les exigences en matière d'instance et les politiques de dimensionnement. Les fournisseurs de capacité servent également de limite de sécurité pour vos fonctions, ce qui signifie que toutes les fonctions attribuées au même fournisseur de capacité doivent faire l'objet d'une confiance mutuelle.

Comportement d'échelle diffère sensiblement des fonctions Lambda traditionnelles. Au lieu d'évoluer à la demande lorsque les appels arrivent, les instances gérées évoluent de manière asynchrone

en fonction de l'utilisation des ressources du processeur. Cette approche élimine les démarrages à froid mais nécessite de planifier la croissance du trafic. Si votre trafic fait plus que doubler en 5 minutes, vous risquez de rencontrer des difficultés à mesure que Lambda augmente sa capacité pour répondre à la demande.

Sécurité et autorisations nécessitent un examen attentif. Vous avez besoin d'autorisations de rôle d'opérateur pour permettre à Lambda de gérer les ressources EC2 de vos fournisseurs de capacité. En outre, les utilisateurs ont besoin du `lambda:PassCapacityProvider` autorisation d'attribuer des fonctions aux fournisseurs de capacité, agissant comme une barrière de sécurité pour contrôler quelles fonctions peuvent être exécutées sur une infrastructure spécifique.

Multi-concurrent exécution est une caractéristique clé des instances gérées. Chaque environnement d'exécution peut gérer plusieurs appels simultanément, maximisant ainsi l'utilisation des ressources pour IO-heavy candidatures. Cela diffère de la méthode Lambda traditionnelle, dans laquelle chaque environnement traite une demande à la fois. Ce modèle d'exécution nécessite une attention particulière à la sécurité des threads, à la gestion des états et à l'isolation du contexte en fonction de votre environnement d'exécution.

Pour plus de détails sur la publication des versions des fonctions auprès de votre fournisseur de capacité, voir the section called “Publication de versions”.

Les sections suivantes fournissent des informations détaillées sur chaque concept de base.

Fournisseurs de capacité

Un fournisseur de capacité constitue la base de l'exécution des instances gérées Lambda. Il constitue la limite de sécurité pour vos fonctions d'événements Lambda et définit les ressources de calcul que Lambda provisionne et gère en votre nom.

Lorsque vous créez un fournisseur de capacité, vous spécifiez :

- Configuration du VPC - Les sous-réseaux et les groupes de sécurité sur lesquels les instances s'exécutent
- Autorisations - Rôles IAM permettant à Lambda de gérer les ressources EC2
- Exigences relatives à l'instance (facultatif) - Architecture et type d'instance préférences
- Configuration de dimensionnement (facultatif) - Comment Lambda fait évoluer vos instances

Comprendre les fournisseurs de capacités en tant que limite de sécurité

Les fournisseurs de capacité constituent la limite de sécurité pour les fonctions Lambda au sein de votre VPC, remplaçant Firecracker-based isolement. Les fonctions s'exécutent dans des conteneurs au sein des instances, mais les conteneurs ne fournissent pas une isolation de sécurité solide entre les fonctions, contrairement aux Firecracker MicroVMS.

Concepts de sécurité clés :

- Fournisseur de capacité : La limite de sécurité qui définit les niveaux de confiance pour les fonctions Lambda
- Isolation des conteneurs : Les conteneurs ne sont PAS un fournisseur de sécurité. Ne vous y fiez pas pour la sécurité entre des charges de travail non fiables
- Séparation de confiance : Séparez les charges de travail qui ne sont pas mutuellement fiables en utilisant différents fournisseurs de capacité

Création d'un fournisseur de capacité

Vous pouvez créer un fournisseur de capacité à l'aide du AWS CLI, AWS Console de gestion, ou AWS SDK.

En utilisant AWS CLI :

```
aws lambda create-capacity-provider \
  --capacity-provider-name my-capacity-provider \
  --vpc-config
 SubnetIds=subnet-12345,subnet-67890,subnet-11111,SecurityGroupIds=sg-12345 \
  --permissions-config CapacityProviderOperatorRoleArn=arn:aws:iam::123456789012:role/
MyOperatorRole \
  --instance-requirements Architectures=x86_64 \
  --capacity-provider-scaling-config ScalingMode=Auto
```

Paramètres requis

CapacityProviderName

- Un nom unique pour votre fournisseur de capacité
- Doit être unique au sein de votre AWS compte

VpcConfig

- SubnetIds (obligatoire) : au moins un sous-réseau, maximum de 16. Utilisez des sous-réseaux dans plusieurs zones de disponibilité pour garantir la résilience
- SecurityGroupIds (facultatif) : groupes de sécurité pour vos instances. Par défaut, le groupe de sécurité par défaut du VPC s'il n'est pas spécifié

PermissionsConfig

- CapacityProviderOperatorRoleArn (obligatoire) : rôle IAM qui permet à Lambda de gérer les ressources EC2 dans votre fournisseur de capacité

Paramètres facultatifs

InstanceRequirements

Spécifiez l'architecture et types d'instances pour votre fournisseur de capacité :

- Architectures: Choisissez `x86_64` ou `arm64`. La valeur par défaut est `x86_64`
- AllowedInstanceTypes: Spécifiez les types d'instances autorisés ou des familles d'instances complètes. Vous pouvez utiliser un caractère générique (`*`) pour correspondre à la taille des instances au sein d'une famille de types d'instances spécifique. Le caractère générique s'applique uniquement à la partie taille (après le point). Par exemple :
  - `m5.8xlarge` — Correspond au type d'instance exact
  - `c6i.*` — Correspond à toutes les tailles du `C6i` famille (`c6i.xlarge`, `c6i.2xlarge`, `c6i.4xlarge`, et ainsi de suite)

  Les caractères génériques sur les familles ou les générations d'instances ne sont pas pris en charge. Par exemple, `c5*.*`, `r*`, et `*3*` ne sont pas des modèles valides pour les instances gérées Lambda.
- ExcludedInstanceTypes: Spécifiez les types d'instances à exclure, en utilisant le même format que AllowedInstanceTypes. Vous ne pouvez spécifier qu'un seul des AllowedInstanceTypes ou ExcludedInstanceTypes.

Par défaut, Lambda choisit les types d'instance optimaux pour votre charge de travail. Nous vous recommandons de laisser les instances gérées Lambda choisir les types d'instance pour vous, car la restriction du nombre de types d'instances possibles peut entraîner une baisse de disponibilité.

CapacityProviderScalingConfig

Configurez la manière dont Lambda fait évoluer vos instances :

- ScalingMode: Réglez sur `Auto` pour une mise à l'échelle automatique ou `Manual` pour le contrôle manuel. La valeur par défaut est `Auto`
- MaxVCpuCount: nombre maximum de vCPU pour le fournisseur de capacité. La valeur par défaut est 400.
- ScalingPolicies: définissez des politiques de dimensionnement du suivi des cibles pour l'utilisation du processeur et de la mémoire

KmsKeyArn

Spécifiez un AWS KMS clé pour le cryptage EBS. La valeur par défaut est AWS clé gérée si elle n'est pas spécifiée.

Balises

Ajoutez des balises pour organiser et gérer vos fournisseurs de capacité.

PropagateTags

Configurez la propagation des balises pour appliquer automatiquement des balises aux ressources gérées (instances Amazon EC2, volumes Amazon EBS et ENI) lancées par le fournisseur de capacité. Utilisez la propagation des balises pour appliquer la répartition des coûts, les SCP et les exigences de conformité. Pour plus d'informations, voir Propagation des balises.

Gestion des fournisseurs de capacités

Mise à jour d’un fournisseur de capacité

Vous pouvez mettre à jour certaines propriétés d'un fournisseur de capacité à l'aide du `UpdateCapacityProvider` API.

```
aws lambda update-capacity-provider \
  --capacity-provider-name my-capacity-provider \
  --capacity-provider-scaling-config ScalingMode=Auto
```

Suppression d’un fournisseur de capacité

Vous pouvez supprimer un fournisseur de capacité lorsqu'il n'est plus nécessaire à l'aide du `DeleteCapacityProvider` API.

```
aws lambda delete-capacity-provider \
  --capacity-provider-name my-capacity-provider
```

Remarque : Vous ne pouvez pas supprimer un fournisseur de capacité auquel sont associées des versions de fonctions.

Affichage des informations sur le fournisseur de capacité

Récupérez des informations sur un fournisseur de capacité à l'aide du `GetCapacityProvider` API.

```
aws lambda get-capacity-provider \
  --capacity-provider-name my-capacity-provider
```

États fournisseurs de capacités

Un fournisseur de capacité peut se trouver dans l'un des états suivants :

- En attente: Le fournisseur de capacités est en cours de création
- Actif: Le fournisseur de capacité est prêt à être utilisé
- Échoué: échec de la création du fournisseur de capacité
- Suppression: Le fournisseur de capacité est en cours de suppression

Quotas

- Capacité maximale de fournisseurs par compte: 1 000
- Nombre maximal de versions de fonctions par fournisseur de capacité: 100 (ne peut pas être augmenté)

Bonnes pratiques

1. Séparer par niveau de confiance: créez différents fournisseurs de capacité pour les charges de travail présentant des exigences de sécurité différentes
2. Utiliser des noms descriptifs: Nommez les fournisseurs de capacités pour indiquer clairement leur utilisation prévue et leur niveau de confiance (par exemple, `production-trusted`, `dev-sandbox`).
3. Utiliser plusieurs zones de disponibilité: Spécifiez des sous-réseaux sur plusieurs zones de disponibilité pour une haute disponibilité

4. Laissez Lambda choisir les types d'instances: sauf si vous avez des exigences matérielles spécifiques, autorisez Lambda à sélectionner les types d'instance optimaux en termes de disponibilité
5. Utilisation du moniteur: Utilisation AWS CloudTrail pour surveiller les affectations et les modèles d'accès des fournisseurs de capacité

Étapes suivantes

- En savoir plus sur mise à l'échelle des instances gérées Lambda
- Comprenez sécurité et autorisations pour les instances gérées Lambda
- Configurez Connectivité VPC pour vos fournisseurs de capacité
- Consultez les guides spécifiques à l'exécution pour Java, Node.js, et Python

Propagation de balises

Avec la propagation des balises, vous pouvez spécifier un ensemble de balises dans la configuration de votre fournisseur de capacité, et Lambda applique automatiquement ces balises à toutes les ressources gérées qu'elle crée, y compris les instances Amazon EC2, les volumes Amazon EBS et les ENI. Cela garantit un balisage cohérent pour la répartition des coûts, les politiques de contrôle des services (SCP) et les exigences de conformité sans intervention manuelle ni automatisation personnalisée.

Configuration de la propagation des balises

Spécifiez le `PropagateTags` paramètre lors de la création ou de la mise à jour d'un fournisseur de capacité à l'aide `UpdateCapacityProvider` des API `CreateCapacityProvider` or.

PropagateTags paramètres :

- Mode (obligatoire) — Mode de propagation des balises :
  - `Explicit`— Propager les balises spécifiées dans dans `ExplicitTags` les ressources gérées.
  - `None`— Désactive la propagation des balises. Aucune balise personnalisée n'est appliquée aux ressources gérées, à l'exception des balises système appliquées par défaut.
- ExplicitTags(obligatoire lorsque Mode est activé`Explicit`) — Une carte de paires clé-valeur à appliquer aux ressources gérées. Vous pouvez spécifier jusqu'à 40 balises.

> **Important**
>
> La propagation des balises s'applique uniquement aux nouvelles ressources gérées mises en service après l'application de la configuration. Les ressources existantes ne sont pas étiquetées rétroactivement.

Exemples

Créez un fournisseur de capacité avec la propagation des balises (AWS CLI) :

```
aws lambda create-capacity-provider \
  --capacity-provider-name my-capacity-provider \
  --vpc-config SubnetIds=subnet-12345,subnet-67890,SecurityGroupIds=sg-12345 \
  --permissions-config CapacityProviderOperatorRoleArn=arn:aws:iam::123456789012:role/
MyOperatorRole \
  --propagate-tags '{"Mode": "Explicit", "ExplicitTags": {"CostCenter": "12345",
 "Environment": "Production"}}'
```

Mettez à jour un fournisseur de capacité existant pour activer la propagation des balises :

```
aws lambda update-capacity-provider \
  --capacity-provider-name my-capacity-provider \
  --propagate-tags '{"Mode": "Explicit", "ExplicitTags": {"CostCenter": "12345",
 "Environment": "Production"}}'
```

Désactiver la propagation des balises :

```
aws lambda update-capacity-provider \
  --capacity-provider-name my-capacity-provider \
  --propagate-tags '{"Mode": "None"}'
```

Comportement de propagation des balises

- Les modifications apportées à `PropagateTags` la configuration n'affectent que les ressources mises en service après la mise à jour. Les ressources déjà lancées conservent leurs balises d'origine.
- Les balises de propagation des balises sont distinctes du `Tags` paramètre indiqué sur le fournisseur de capacité lui-même. Les balises de fournisseur de capacité identifient la ressource

du fournisseur de capacité ; les balises propagées sont appliquées aux ressources gérées que le fournisseur de capacité lance.

- Les balises propagées sont prises en compte dans les limites AWS des balises de ressources sur les ressources cibles.

Mise à l'échelle des instances gérées Lambda

Les instances gérées Lambda ne sont pas évolutives lorsque les appels arrivent et ne prennent pas en charge les démarrages à froid. Au lieu de cela, il évolue de manière asynchrone à l'aide de signaux de consommation de ressources. Les instances gérées évoluent actuellement en fonction de l'utilisation des ressources du processeur et de la saturation multisimultanéité.

Principales différences :

- Lambda (par défaut) : évolue lorsqu'il n'existe pas d'environnement d'exécution libre pour gérer une invocation entrante (démarrage à froid)
- Instances gérées Lambda : évolue de manière asynchrone en fonction de l'utilisation des ressources du processeur et de la saturation multisimultanée des environnements d'exécution

Si votre trafic fait plus que doubler en 5 minutes, vous risquez de rencontrer des problèmes à mesure que Lambda fait évoluer les instances et les environnements d'exécution pour répondre à la demande.

Le cycle de vie du dimensionnement

Les instances gérées Lambda utilisent une architecture distribuée pour gérer la mise à l'échelle :

Composantes :

- Instances gérées : exécutées sur votre compte dans les sous-réseaux que vous fournissez
- Routeur et scaler : composants Lambda partagés qui acheminent les appels et gèrent la mise à l'échelle
- Agent Lambda : s'exécute sur chaque instance gérée pour gérer le cycle de vie de l'environnement d'exécution et surveiller la consommation des ressources

Comment ça fonctionne :

1. Lorsque vous publiez une version de fonction avec un fournisseur de capacité, Lambda lance des instances gérées dans votre compte. Il en lance trois par défaut pour la résilience AZ et démarre trois environnements d'exécution avant de marquer la version de votre fonction comme ACTIVE.
2. Chaque instance gérée peut exécuter des environnements d'exécution pour plusieurs fonctions mappées au même fournisseur de capacité.
3. Au fur et à mesure que le trafic entre dans votre application, les environnements d'exécution consomment des ressources. L'agent Lambda informe le Scaler, qui décide s'il convient de dimensionner de nouveaux environnements d'exécution ou des instances gérées.
4. Si Router tente d'envoyer une invocation à un environnement d'exécution consommant beaucoup de ressources, l'agent Lambda de cette instance lui demande de réessayer sur une autre.
5. Lorsque le trafic diminue, l'agent Lambda en informe Scaler, qui prend la décision de réduire les environnements d'exécution et de déployer les instances gérées.

Ajustement du comportement de dimensionnement

Vous pouvez personnaliser le comportement de dimensionnement des instances gérées à l'aide de cinq contrôles :

Contrôles au niveau des fonctions

1. Mémoire de fonctions et processeurs virtuels

Choisissez la taille de la mémoire et l'allocation du processeur virtuel pour votre fonction. La plus petite taille de fonction prise en charge est de 2 Go et 1 vCPU.

Considérations :

- Choisissez un paramètre de mémoire et de processeur virtuel qui prend en charge les exécutions multisimultanées de votre fonction
- Vous ne pouvez pas configurer une fonction avec moins d'un processeur virtuel car les fonctions exécutées sur des instances gérées doivent prendre en charge des charges de travail multisimultanées
- Vous ne pouvez pas choisir moins de 2 Go car cela correspond au ratio mémoire/processeur virtuel de 2 pour 1 des instances c, qui présentent le ratio le plus faible
- Pour les applications Python, vous devrez peut-être choisir un ratio plus élevé entre la mémoire et les processeurs virtuels, par exemple 4 pour 1 ou 8 pour 1, en raison de la façon dont Python gère la multisimultanéité

- Si vous exécutez des CPU-intensive opérations ou si vous effectuez peu d'E/S, vous devez choisir plusieurs processeurs virtuels

2. Simultanéité maximum

Définissez la simultanéité maximale par environnement d'exécution.

Comportement par défaut : Lambda choisit des valeurs par défaut judicieuses qui équilibrent la consommation de ressources et le débit, ce qui convient à une grande variété d'applications.

Directives d'ajustement :

- Augmenter la simultanéité : si vos appels de fonctions utilisent très peu de processeur, vous pouvez augmenter la simultanéité maximale jusqu'à un maximum de 64 par processeur virtuel
- Diminuer la simultanéité : si votre application consomme une grande quantité de mémoire et très peu de processeur, vous pouvez réduire votre simultanéité maximale

Important : étant donné que les instances gérées Lambda sont destinées à des applications multisimultanées, les environnements d'exécution présentant une très faible simultanéité peuvent rencontrer des contraintes lors de la mise à l'échelle. Lorsque les appels arrivent dans un environnement d'exécution qui a atteint sa limite de simultanéité, Lambda achemine ces appels ailleurs et développe de nouveaux environnements d'exécution pour gérer la charge. Pour identifier la contrainte de ressources à l'origine des ralentissements, surveillez les métriques des raisons de l'étranglement (`ConcurrencyThrottles`, `CPUThrottlesMemoryThrottles`, et`DiskThrottles`) décrites dans. Types de métriques pour les fonctions d'événement Lambda

3. Environnements d'exécution par fonction

Définissez le nombre minimum et maximum d'environnements d'exécution pour votre fonction.

Comportement par défaut : le minimum par défaut est de 3 environnements d'exécution répartis dans les zones de disponibilité, sans maximum par défaut. Vous pouvez remplacer les deux valeurs une fois la fonction créée.

Directives d'ajustement :

- Définissez le minimum : prévoyez de la capacité pour le trafic de base et réduisez les gaz en cas de rafales soudaines. Les valeurs inférieures à 3 réduisent la redondance de la zone de disponibilité.

- Définissez le maximum : plafonnez le nombre d'environnements d'exécution pour contrôler la scale-out et éviter les problèmes de voisinage bruyants lorsque plusieurs fonctions partagent un fournisseur de capacité.
- Désactiver la fonction : réglez à la fois le minimum et le maximum sur 0 pour désactiver une fonction sans la supprimer.

Exemple :

```
aws lambda put-function-scaling-config \
  --function-name my-lmi-function \
  --qualifier '$LATEST.PUBLISHED' \
  --function-scaling-config MinExecutionEnvironments=5,MaxExecutionEnvironments=20 \
  --region us-east-1
```

Remarques importantes :

- Portée du qualificatif : ces configurations s'appliquent au niveau de la fonction pour chaque ARN qualifié. Lorsque cette option est activée`$LATEST.PUBLISHED`, la configuration se propage aux `$LATEST.PUBLISHED` versions futures. Lorsqu'elles sont définies sur une version spécifique, les nouvelles versions publiées reviennent aux valeurs par défaut.
- Configuration couplée : vous devez définir les valeurs minimale et maximale ensemble. Tout paramètre non spécifié revient à sa valeur par défaut. Les valeurs sont valides pour les deux `MinExecutionEnvironments` et sont `MaxExecutionEnvironments` comprises entre 0 et 15 000. Un minimum de 0 n'est valide que si le maximum est également égal à 0.
- Incidence financière : la désactivation de la fonction prend effet au niveau de la version de la fonction. Lambda met fin à une instance EC2 sous-jacente lorsqu'aucun environnement d'exécution n'est actif, et les frais d'instance se poursuivent jusqu'à la fin de la résiliation (généralement en quelques minutes).

Contrôles au niveau des fournisseurs de capacité

4. Utilisation des ressources cible

Choisissez votre propre objectif en matière de consommation d'utilisation du processeur.

Comportement par défaut : Lambda conserve une marge de manœuvre suffisante pour que votre trafic double en 5 minutes sans ralentissement.

Options d'optimisation :

- Si votre charge de travail est très stable ou si votre application n'est pas sensible aux contraintes, vous pouvez fixer l'objectif à un niveau élevé afin d'augmenter le taux d'utilisation et de réduire les coûts
- Si vous souhaitez conserver une marge de manœuvre en cas de rafales de trafic, vous pouvez définir des objectifs de ressources à un niveau bas, ce qui nécessite davantage de capacité

5. Sélection du type d'instance

Définissez les types d'instances autorisés ou exclus.

Comportement par défaut : Lambda choisit les types d'instances les mieux adaptés à votre charge de travail. Il est recommandé de laisser les instances gérées Lambda choisir les types d'instance, car la limitation du nombre de types d'instances possibles peut entraîner une baisse de la disponibilité.

Configuration personnalisée :

- Configuration matérielle spécifique : définissez les types d'instances autorisés sur une liste d'instances compatibles. Par exemple, si votre application nécessite une bande passante réseau élevée, vous pouvez sélectionner plusieurs types d'instances n
- Optimisation des coûts : pour les environnements de test ou de développement, vous pouvez choisir des types d'instances plus petits, tels que les types d'instance m7a.large

Mise à l'échelle planifiée

Utilisez Amazon EventBridge Scheduler pour ajuster les environnements d'exécution minimum et maximum de votre fonction selon un calendrier récurrent ou ponctuel. Cela est utile pour des modèles de trafic prévisibles, tels que la mise à l'échelle avant les heures de pointe et la réduction pendant les heures creuses.

Configuration du planificateur :

- Créez un rôle d'exécution du EventBridge planificateur ou utilisez un rôle existant qui autorise l'appel à votre `lambda:PutFunctionScalingConfig` fonction cible.
- Créez un calendrier à l'aide d'une expression cron ou rate, en ciblant l'`PutFunctionScalingConfig`API en tant que cible universelle. Spécifiez les nouvelles `MaxExecutionEnvironments` valeurs `MinExecutionEnvironments` et dans la charge utile d'entrée.

Exemple 1 : évolutivité pour gérer les pics de trafic planifiés

Créez deux horaires pour augmenter l'échelle avant les heures de pointe et la réduire par la suite. Chaque calendrier cible l'`PutFunctionScalingConfig`API avec des `MaxExecutionEnvironments` valeurs `MinExecutionEnvironments` et mises à jour.

Passez à la vitesse supérieure à 8 h 00 UTC (min = 100, max = 1000) :

```
aws scheduler create-schedule \
  --name "ScaleUpLambdaManagedInstances" \
  --schedule-expression "cron(0 8 * * ? *)" \
  --flexible-time-window '{"Mode": "OFF"}' \
  --target '{
    "Arn": "arn:aws:scheduler:::aws-sdk:lambda:PutFunctionScalingConfig",
    "RoleArn": "arn:aws:iam::<account-id>:role/eventbridge-scheduler-role",
    "Input": "{\"FunctionName\": \"my-lmi-function\", \"Qualifier\":
 \"$LATEST.PUBLISHED\", \"FunctionScalingConfig\": {\"MinExecutionEnvironments\": 100,
 \"MaxExecutionEnvironments\": 1000}}"
  }'
```

Réduisez la taille à 18 h 00 UTC (min = 5, max = 20) :

```
aws scheduler create-schedule \
  --name "ScaleDownLambdaManagedInstances" \
  --schedule-expression "cron(0 18 * * ? *)" \
  --flexible-time-window '{"Mode": "OFF"}' \
  --target '{
    "Arn": "arn:aws:scheduler:::aws-sdk:lambda:PutFunctionScalingConfig",
    "RoleArn": "arn:aws:iam::<account-id>:role/eventbridge-scheduler-role",
    "Input": "{\"FunctionName\": \"my-lmi-function\", \"Qualifier\":
 \"$LATEST.PUBLISHED\", \"FunctionScalingConfig\": {\"MinExecutionEnvironments\": 5,
 \"MaxExecutionEnvironments\": 20}}"
  }'
```

Exemple 2 : désactiver en dehors des heures de pointe et réactiver

Le réglage des deux `MinExecutionEnvironments` et `MaxExecutionEnvironments` sur 0 désactive la version de la fonction sans la supprimer. Une fonction désactivée n'est pas automatiquement redimensionnée en fonction du trafic. Vous devez le réactiver explicitement en définissant des valeurs non nulles par le biais d'une autre action planifiée.

Désactiver à 22 h UTC (min = 0, max = 0) :

```
aws scheduler create-schedule \
  --name "DeactivateLambdaManagedInstances" \
  --schedule-expression "cron(0 22 * * ? *)" \
  --flexible-time-window '{"Mode": "OFF"}' \
  --target '{
    "Arn": "arn:aws:scheduler:::aws-sdk:lambda:PutFunctionScalingConfig",
    "RoleArn": "arn:aws:iam::<account-id>:role/eventbridge-scheduler-role",
    "Input": "{\"FunctionName\": \"my-lmi-function\", \"Qualifier\":
 \"$LATEST.PUBLISHED\", \"FunctionScalingConfig\": {\"MinExecutionEnvironments\": 0,
 \"MaxExecutionEnvironments\": 0}}"
  }'
```

Réactivez à 7 h 00 UTC (min = 10, max = 20) :

```
aws scheduler create-schedule \
  --name "ReactivateLambdaManagedInstances" \
  --schedule-expression "cron(0 7 * * ? *)" \
  --flexible-time-window '{"Mode": "OFF"}' \
  --target '{
    "Arn": "arn:aws:scheduler:::aws-sdk:lambda:PutFunctionScalingConfig",
    "RoleArn": "arn:aws:iam::<account-id>:role/eventbridge-scheduler-role",
    "Input": "{\"FunctionName\": \"my-lmi-function\", \"Qualifier\":
 \"$LATEST.PUBLISHED\", \"FunctionScalingConfig\": {\"MinExecutionEnvironments\": 10,
 \"MaxExecutionEnvironments\": 20}}"
  }'
```

Directives d'ajustement :

- Pour les charges de travail dont les pics sont prévisibles, créez plusieurs programmes en fonction de votre trafic : un pour augmenter votre fonction avant les heures de pointe, et un autre pour le réduire après les heures de pointe. Chaque calendrier suit le même schéma avec des `MaxExecutionEnvironments` valeurs `MinExecutionEnvironments` et mises à jour.
- La mise à l'échelle planifiée ajuste le plancher et le plafond prévus pour les environnements d'exécution, mais la mise à l'échelle réelle entre min et max dépend toujours de l'utilisation du processeur et de la saturation de la simultanéité.
- Si votre trafic fait plus que doubler dans les 5 minutes suivant une augmentation planifiée, il se peut que vous rencontriez encore des difficultés lors de l'approvisionnement de la capacité.
- Lorsque vous passez à zéro pour désactiver une fonction, n'oubliez pas que la réactivation nécessite un `PutFunctionScalingConfig` appel explicite avec des valeurs différentes de zéro.

Étapes suivantes

- En savoir plus sur les fournisseurs de capacité pour les instances gérées Lambda
- Consultez les guides spécifiques à l'exécution pour gérer la multisimultanéité
- Configurez la connectivité VPC pour vos fournisseurs de capacité
- Surveillez les mesures de dimensionnement pour optimiser le comportement de dimensionnement

Sécurité et autorisations

Les instances gérées Lambda utilisent des fournisseurs de capacité comme limites de confiance. Les fonctions d'événement Lambda s'exécutent dans des conteneurs au sein de ces instances, mais les conteneurs ne fournissent pas d'isolation de sécurité entre les charges de travail. Toutes les fonctions assignées au même fournisseur de capacité doivent être mutuellement fiables.

Concepts de sécurité clés

- Fournisseur de capacité : limite de sécurité qui définit les niveaux de confiance pour les fonctions Lambda
- Isolation des conteneurs : les conteneurs ne constituent pas une limite de sécurité. Ne vous fiez pas à eux pour assurer la sécurité entre des charges de travail non fiables
- Séparation de confiance : Séparez les charges de travail qui ne sont pas mutuellement fiables en utilisant différents fournisseurs de capacité

Autorisations nécessaires

PassCapacityProvider Action

Les utilisateurs doivent être `lambda:PassCapacityProvider` autorisés à attribuer des fonctions aux fournisseurs de capacité. Cette autorisation agit comme une barrière de sécurité, garantissant que seuls les utilisateurs autorisés peuvent confier des fonctions à des fournisseurs de capacité spécifiques.

Les administrateurs de compte contrôlent les fonctions qui peuvent utiliser des fournisseurs de capacité spécifiques par le biais de l'action `lambda:PassCapacityProvider` IAM. Cette action est requise dans les cas suivants :

- Création de fonctions utilisant des instances gérées Lambda
- Mettre à jour les configurations des fonctions pour utiliser un fournisseur de capacité

- Déploiement de fonctions en utilisant l'infrastructure comme code

Exemple de politique IAM

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "lambda:PassCapacityProvider",
      "Resource": "arn:aws:lambda:*:*:capacity-provider:trusted-workloads-*"
    }
  ]
}
```

Service-Linked Rôle

AWS Lambda utilise le rôle `AWSServiceRoleForLambda` lié au service pour gérer les ressources ec2 des instances gérées Lambda auprès de vos fournisseurs de capacité.

Bonnes pratiques

1. Séparation par niveau de confiance : créez différents fournisseurs de capacité pour les charges de travail ayant des exigences de sécurité différentes
2. Utiliser des noms descriptifs : nommez les fournisseurs de capacité pour indiquer clairement leur utilisation prévue et leur niveau de confiance (par exemple`production-trusted`,`dev-sandbox`)
3. Appliquer le moindre privilège : octroyer `PassCapacityProvider` des autorisations uniquement aux fournisseurs de capacité nécessaires
4. Surveiller l'utilisation : AWS CloudTrail à utiliser pour surveiller les attributions des fournisseurs de capacité et les modèles d'accès

Étapes suivantes

- En savoir plus sur les fournisseurs de capacité pour les instances gérées Lambda
- Comprendre le dimensionnement pour les instances gérées Lambda
- Configurez la connectivité VPC pour vos fournisseurs de capacité
- Consultez les guides spécifiques à l'exécution pour Java et Node.jsPython

Rôle d'opérateur Lambda pour les instances gérées Lambda

Lorsque vous utilisez des instances gérées Lambda, Lambda a besoin d'autorisations pour gérer la capacité de calcul de votre compte. Le rôle d'opérateur fournit ces autorisations via des politiques IAM qui permettent à Lambda de gérer les instances EC2 dans le fournisseur de capacité.

Lambda assume le rôle d'opérateur lors de l'exécution de ces opérations de gestion, de la même manière que Lambda assume un rôle d'exécution lorsque votre fonction d'événement Lambda s'exécute.

Création d'un rôle d'opérateur

Vous pouvez créer un rôle d'opérateur dans la console IAM ou à l'aide de la AWS CLI. Le rôle doit inclure :

- Politique d'autorisations : accorde des autorisations pour gérer les fournisseurs de capacité et les ressources associées
- Politique de confiance — Permet au service Lambda (`lambda.amazonaws.com`) d'assumer le rôle

Politique d’autorisations

Le rôle d'opérateur nécessite des autorisations pour gérer les fournisseurs de capacité et les ressources informatiques sous-jacentes. Au minimum, le rôle nécessite les autorisations définies dans la politique AWSLambdaManagedEC2ResourceOperatorgérée, actuellement :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:RunInstances",
        "ec2:CreateTags",
        "ec2:AttachNetworkInterface"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
```

```
      "Condition": {
        "StringEquals": {
          "ec2:ManagedResourceOperator": "scaler.lambda.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEncryptionControls"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:RunInstances",
        "ec2:CreateNetworkInterface"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:RunInstances"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition": {
        "StringEquals": {
          "ec2:Owner": "amazon"
        }
```

```
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup"
      ],
      "Resource": "arn:aws:logs:*:*:log-group:*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource": "arn:aws:logs:*:*:log-group:*:log-stream:*"
    }
  ]
}
```

Politique d’approbation

La politique de confiance permet à Lambda d'assumer le rôle d'opérateur :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Service-Linked Rôle des instances gérées Lambda

Pour gérer de manière responsable le cycle de vie des instances gérées Lambda, Lambda a besoin d'un accès permanent pour mettre fin aux instances gérées de votre compte. Lambda utilise un rôle lié à un service (SLR) AWS Identity and Access Management (IAM) pour effectuer ces opérations.

Création automatique : le rôle lié au service est automatiquement créé la première fois que vous créez un fournisseur de capacité. L'utilisateur qui crée le premier fournisseur de capacité doit avoir l'`iam:CreateServiceLinkedRole`autorisation pour le `lambda.amazonaws.com` principal.

Autorisations : le rôle lié au service accorde à Lambda les autorisations suivantes sur les instances gérées :

- `ec2:TerminateInstances`— Pour mettre fin aux instances à la fin de leur cycle de vie
- `ec2:DescribeInstances`— Pour énumérer les instances gérées

Suppression : vous ne pouvez supprimer ce rôle lié à un service qu'après avoir supprimé tous les fournisseurs de capacité des instances gérées Lambda de votre compte.

Pour plus d'informations sur les rôles liés à un service, consultez the section called “Utilisation des rôles liés à un service”.

Comprendre l'environnement d'exécution des instances gérées Lambda

Les instances gérées Lambda fournissent un modèle de déploiement alternatif qui exécute votre code de fonction sur les instances Amazon EC2 appartenant au client, tandis que Lambda gère les aspects opérationnels. L'environnement d'exécution des instances gérées présente plusieurs différences importantes par rapport aux fonctions Lambda (par défaut), notamment en ce qui concerne la façon dont il gère les appels simultanés et les cycles de vie des conteneurs.

Remarque : Pour plus d'informations sur l'environnement d'exécution Lambda (par défaut), voir Comprendre le cycle de vie de l'environnement d'exécution Lambda.

Cycle de vie des environnements d'exécution

Le cycle de vie d'un environnement d'exécution de fonctions Lambda Managed Instances diffère de celui de Lambda (par défaut) de plusieurs manières principales :

Phase d'initialisation

Pendant la phase d'initialisation, Lambda exécute les étapes suivantes :

- Initialisez et enregistrez toutes les extensions
- Bootstrap le point d'entrée d'exécution. L'exécution génère le nombre configuré de travailleurs d'exécution (la mise en œuvre dépend de l'exécution)

- Exécuter le code d'initialisation de la fonction (code en dehors du gestionnaire)
- Attendez qu'au moins un agent d'exécution signale qu'il est prêt en appelant `/runtime/invocation/next`

La phase d'initialisation est considérée comme terminée lorsque les extensions sont initialisées et qu'au moins un agent d'exécution a appelé. `/runtime/invocation/next` La fonction est alors prête à traiter les invocations.

> **Note**
>
> Pour les fonctions Lambda Managed Instances, l'initialisation peut prendre jusqu'à 15 minutes. Le délai d'attente est de 130 secondes au maximum ou du délai d'expiration de la fonction configurée (jusqu'à 900 secondes).

Phase d’invocation

La phase d'appel pour les fonctions Lambda Managed Instances présente plusieurs caractéristiques uniques :

Fonctionnement en continu Contrairement à Lambda (par défaut), l'environnement d'exécution reste actif en permanence, traitant les appels au fur et à mesure qu'ils arrivent sans se figer entre les appels.

Traitement en parallèle. Plusieurs invocations peuvent être exécutées simultanément dans le même environnement d'exécution, chacune étant gérée par un agent d'exécution différent.

Délais d'attente indépendants. Le délai d'expiration configuré pour la fonction s'applique à chaque appel individuel. Lorsqu'un appel expire, Lambda marque cet appel spécifique comme ayant échoué, mais n'interrompt pas les autres appels en cours et ne met pas fin à l'environnement d'exécution.

Gestion de la contre-pression. Si tous les travailleurs d'exécution sont occupés à traiter les invocations, les nouvelles demandes d'invocation sont rejetées jusqu'à ce qu'un travailleur soit disponible.

Gestion des erreurs et restauration

La gestion des erreurs dans les environnements d'exécution des fonctions des instances gérées Lambda diffère de celle de Lambda (par défaut) :

Pannes du Runtime Worker. Si un processus d'exécution tombe en panne, l'environnement d'exécution continue de fonctionner avec les autres travailleurs sains.

L'extension se bloque. Si un processus d'extension se bloque pendant l'initialisation ou le fonctionnement, l'ensemble de l'environnement d'exécution est marqué comme défectueux et est arrêté. Lambda crée un nouvel environnement d'exécution pour le remplacer.

Non reset/repair Contrairement à Lambda (par défaut), les instances gérées ne tentent pas de réinitialiser et de réinitialiser l'environnement d'exécution après des erreurs. Au lieu de cela, les contenants insalubres sont retirés et remplacés par de nouveaux.

Invoquer des délais

Lorsqu'une invocation individuelle expire, Lambda renvoie une `Task timed out after <timeout> seconds` erreur avec un statut d'erreur de fonction à l'appelant. Toutefois, les instances gérées Lambda ne mettent pas fin de force à votre code : il continue de s'exécuter dans l'environnement d'exécution. En tant que développeur de fonctions, vous êtes responsable de la détection et de la gestion du délai d'attente.

L'objet de contexte indique le temps restant pour l'invocation. Une valeur nulle ou négative indique que le délai d'invocation a expiré. Les autres appels simultanés dans l'environnement d'exécution continuent à être traités normalement.

Comportement de nouvelle tentative

Lorsqu'une invocation expire :

- Invocations synchrones : l'appelant reçoit l'erreur de temporisation et est chargé de réessayer.
- Invocations asynchrones : Lambda réessaie en fonction de la politique de nouvelle tentative de votre fonction (par défaut : 2 tentatives). Une fois toutes les tentatives épuisées, l'événement est envoyé vers la file d'attente de lettres mortes configurée ou vers la destination en cas d'échec, le cas échéant.
- Mappages de sources d'événements : le comportement des nouvelles tentatives dépend de la configuration de la source d'événements (par exemple, taille du lot, bissection en cas d'erreur, nombre maximum de tentatives). Le lot peut être réessayé ou envoyé vers une destination en cas d'échec en fonction de vos politiques en matière de nouvelles tentatives.

Que se passe-t-il si vous ne gérez pas le délai d'attente

Si votre code ne vérifie pas le temps restant et arrête l'exécution :

- L'invocation est déjà marquée comme ayant échoué. Lambda a déjà renvoyé une erreur de temporisation à l'appelant : tout travail effectué par votre code après le délai est effectivement perdu du point de vue de l'appelant.
- Les ressources restent consommées. Votre code continue d'occuper un emplacement de travail d'exécution, ce qui réduit la simultanéité disponible pour les nouvelles invocations sur cette instance.
- Comportement non déterministe. Votre code ne s'arrête pas lorsque le timeout se déclenche : il continue de s'exécuter en arrière-plan. Cela signifie que des effets secondaires peuvent encore survenir même si Lambda a déjà informé l'appelant que l'appel avait échoué.

  Par exemple, votre gestionnaire écrit un enregistrement dans DynamoDB, puis le délai d'attente se déclenche et Lambda renvoie une erreur de temporisation à l'appelant, mais votre code est toujours en cours d'exécution et envoie une notification SNS. L'appelant tente à nouveau l'invocation, qui écrit à nouveau l'enregistrement et envoie à nouveau la notification. Vous avez maintenant des données dupliquées et des notifications dupliquées, et il n'est pas facile de savoir lesquelles provenaient de l'appel « échoué » qui était toujours en cours d'exécution en arrière-plan.

Gestion des délais d'attente dans votre code

Utilisez l'objet de contexte pour vérifier le temps restant et arrêter le traitement avant le délai imparti. Configurez une mémoire tampon en fonction de la durée prévue de votre prochaine unité de travail. Par exemple, si le traitement de chaque élément prend environ 500 ms, réglez la mémoire tampon sur au moins 500 ms plus la marge.

Pour des exemples de gestion du délai d'attente spécifiques à la langue, consultez la section sur le contexte de la demande de chaque page d'exécution :

- Node.js contexte de la demande
- Contexte de requête Python
- Contexte de requête Java
- Contexte de requête .NET

Lazy-load images de conteneurs avec Seekable OCI (SOCI)

Pour les fonctions événementielles Lambda déployées sous forme d'images de conteneur sur des instances gérées Lambda, Lambda télécharge et décompresse l'image sur chaque instance avant de démarrer un environnement d'exécution. Pour les images de grande taille, cette extraction représente

la plus grande partie du temps entre la publication d'une version de fonction ou sa mise à l'échelle et le moment où l'environnement d'exécution gère sa première invocation. Avec Seekable OCI (SOCI), Lambda peut démarrer l'environnement d'exécution avant que l'ensemble de l'image ne soit téléchargé.

SOCI est un technologie open source développé par AWS. Il utilise un index qui fait correspondre chaque fichier de l'image à son emplacement dans les couches de l'image. Lambda utilise l'index pour récupérer uniquement les fichiers à la demande au fur et à mesure que votre fonction les lit, au lieu de télécharger et de déballer l'image complète avant de démarrer le conteneur. Les images de conteneur regroupent généralement de vastes ensembles de bibliothèques et de dépendances, qui ne sont pas toutes lues au démarrage ou lors d'une seule invocation. Le chargement différé en tire parti en récupérant uniquement ce que votre fonction lit réellement, ce qui réduit le délai de première invocation et rend le temps de démarrage beaucoup moins sensible à la taille totale de l'image. L'avantage est le plus important pour les images de plusieurs gigaoctets où votre fonction ne lit qu'un sous-ensemble du contenu par appel, comme les images qui regroupent des frameworks d'apprentissage automatique.

Comment fonctionne SOCI sur les instances gérées Lambda

1. Vous créez un index SOCI pour votre image et vous l'envoyez à Amazon ECR à côté de l'image. Le résultat est un index d'images de l'Open Container Initiative (OCI) qui fait référence à deux artefacts : votre manifeste d'image d'origine et l'index SOCI.
2. Vous créez ou mettez à jour votre fonction avec un URI d'image qui pointe vers l'index de l'image. Lambda détecte l'index SOCI et active le chargement différé pour les environnements d'exécution de cette fonction. Vous n'avez pas besoin de modifier la configuration d'une autre fonction.
3. Lambda extrait le contenu des images à la demande. Les fichiers lus par votre code d'initialisation sont récupérés lors de l'initialisation. Les fichiers que votre gestionnaire lit pour la première fois sont récupérés lors de cette invocation. Lambda ne télécharge pas le reste de l'image en arrière-plan.

> **Note**
>
> Si votre fonction lit un fichier pour la première fois lors d'une invocation plutôt que pendant l'initialisation, Lambda récupère ce fichier lors de la première invocation, ce qui augmente la durée de cette invocation. Pour garantir la cohérence des durées d'invocation, importez toutes les bibliothèques et lisez tous les fichiers dont votre fonction a besoin dans votre code d'initialisation, et non dans le gestionnaire. Nous vous recommandons de tester votre fonction

avec et sans SOCI afin de comparer le temps de démarrage et la durée d'invocation de votre charge de travail.

Créez un index SOCI pour votre image

L'exemple suivant s'exécute sur Amazon Linux 2023. Il installe le snapshotter SOCI, containerd et nerdctl, puis crée un index SOCI pour une image existante dans Amazon ECR et affiche le résultat. Remplacez les valeurs des espaces réservés par les vôtres. Pour d'autres méthodes de création et de diffusion d'un index SOCI, voir Premiers pas avec le snapshotter SOCI sur GitHub.

```
sudo yum install -y soci-snapshotter containerd nerdctl
sudo systemctl start soci-snapshotter
sudo systemctl restart containerd

ACCOUNT_ID="111122223333"
REGION="us-east-2"
REPOSITORY_NAME="my-function"
ORIGINAL_IMAGE_TAG="v1"
SOCI_IMAGE_TAG="v1-soci"
REGISTRY="$ACCOUNT_ID.dkr.ecr.$REGION.amazonaws.com"

aws ecr get-login-password --region $REGION | sudo nerdctl login -u AWS --password-
stdin $REGISTRY

sudo nerdctl pull $REGISTRY/$REPOSITORY_NAME:$ORIGINAL_IMAGE_TAG
sudo nerdctl image convert --soci $REGISTRY/$REPOSITORY_NAME:$ORIGINAL_IMAGE_TAG
 $REGISTRY/$REPOSITORY_NAME:$SOCI_IMAGE_TAG
sudo nerdctl push --platform linux/arm64 $REGISTRY/$REPOSITORY_NAME:$SOCI_IMAGE_TAG
```

Note

Cet exemple crée un `arm64` (AWS Image (graviton). Lambda ne prend en charge que les images de conteneurs à architecture unique. Votre image doit donc cibler une architecture de jeu d'instructions unique, et `--platform` la valeur doit correspondre à l'architecture de votre fonction. Pour plus d’informations, consultez the section called “Kits d'instructions (ARM/x86)”.

Utiliser `$REGISTRY/$REPOSITORY_NAME:$SOCI_IMAGE_TAG` comme URI de l'image lorsque vous créez ou mettez à jour votre fonction. Publiez ensuite une version de la fonction. Lambda résout la version de la fonction en index d'image et active le chargement différé.

Exigences et limitations

Version de l'indice SOCI

Lambda prend en charge SOCI Index Manifest v2 uniquement (type de média) `application/vnd.amazon.soci.index.v2+json`). Lambda ne prend pas en charge les index SOCI Index Manifest v1. Le `nerdctl image convert --soci` La commande de la section précédente produit un index v2.

Format d'index d'image

L'index d'images doit contenir exactement deux entrées : l'index SOCI et un manifeste d'image OCI.

URI de l’image

Pointez l'URI de l'image de votre fonction vers SOCI-indexed tag (par exemple, `my-function:v1-soci`), pas sur la balise d'image d'origine. Lambda résout la version de la fonction en index d'image. Pour modifier l'image ou l'index, appuyez sur une nouvelle SOCI-indexed balise et met à jour l'URI de l'image de la fonction.

Disponibilité

SOCI est disponible uniquement pour les fonctions d'image de conteneur exécutées sur des instances gérées Lambda.

$ LATEST.PUBLISHED version dans les instances gérées Lambda

Les fonctions Lambda Managed Instances prennent en charge le même flux de travail de versionnage numéroté que Lambda (par défaut). Si vous préférez ne pas gérer les versions numérotées, Lambda Managed Instances introduit un nouveau type de version :`$LATEST.PUBLISHED`. Avec ce type de version, vous pouvez créer ou republier une version publiée avec un code ou une configuration mis à jour. Il n'est pas nécessaire de gérer les versions numérotées.

Différence clé par rapport à $LATEST : lorsque vous invoquez une fonction Lambda Managed Instances à l'aide d'un ARN non qualifié, Lambda invoque implicitement la version plutôt que la `$LATEST.PUBLISHED` version non publiée $LATEST.

La commande AWS CLI suivante crée ou republie la `$LATEST.PUBLISHED` version.

```
aws lambda publish-version --function-name my-function --publish-to LATEST_PUBLISHED
```

Vous devriez voir la sortie suivante :

```
{
  "FunctionName": "my-function",
  "FunctionArn": "arn:aws:lambda:us-east-2:123456789012:function:my-function:
$LATEST.PUBLISHED",
  "Version": "$LATEST.PUBLISHED",
  "Role": "arn:aws:iam::123456789012:role/lambda-role",
  "Handler": "function.handler",
  "Runtime": "nodejs24.x",
  ...
}
```

> **Note**
>
> Si vous utilisez AWS CloudFormation ou la console Lambda pour créer une fonction Lambda Managed Instances, Lambda crée automatiquement la version. `$LATEST.PUBLISHED`

Déploiement et mise à jour des fonctions des instances gérées Lambda

Lorsque vous mettez à jour une fonction Lambda Managed Instances, Lambda provisionne des environnements d'exécution pour la nouvelle version de la fonction sur vos instances gérées avant de transférer le trafic vers celle-ci. Vous pouvez contrôler la vitesse et la sécurité du déploiement en sélectionnant une stratégie de déploiement. Cette rubrique décrit les stratégies de déploiement disponibles pour les fonctions Lambda Managed Instances et explique comment les définir avec l'infrastructure en tant que code (IaC).

> **Note**
>
> Avant de déployer une fonction, vous devez disposer d'un fournisseur de capacité. Pour plus d'informations, voir fournisseurs de capacité pour les instances gérées Lambda.

Stratégies de déploiement

Les instances gérées Lambda prennent en charge les stratégies suivantes pour publier une nouvelle version de fonction. Choisissez la stratégie qui correspond au niveau de contrôle que vous souhaitez conserver pendant le déploiement. Les mises à jour continues sont l'option la plus simple. Blue/green et les déploiements de Canary vous permettent de mieux contrôler la façon dont le trafic est transféré vers la nouvelle version.

Mises à jour continues

Pour effectuer une mise à jour continue, vous publiez vos modifications dans le `$LATEST.PUBLISHED` version de votre fonction. `$LATEST.PUBLISHED` est un type de version spécifique aux instances gérées Lambda que vous republiez avec un nouveau code ou une nouvelle configuration au lieu de conserver des versions numérotées. Lorsque vous appelez une fonction Lambda Managed Instances avec son Amazon Resource Name (ARN) non qualifié, Lambda invoque `$LATEST.PUBLISHED` version. Pour plus d'informations, consultez the section called “Publication de versions”.

Chaque fois que vous republiez `$LATEST.PUBLISHED`, Lambda remplace progressivement les environnements d'exécution de vos instances gérées par la nouvelle version, sans que vous ayez à gérer le transfert du trafic directement via un alias de fonction. Il s'agit de la stratégie la plus simple.

Utilisez les mises à jour continues lorsque vous souhaitez un transfert progressif automatique du trafic de l'ancienne version vers la nouvelle version, et que vous n'avez pas besoin de contrôler directement le pourcentage de trafic envoyé à chaque version pour gérer le déploiement ou la restauration.

Blue/green déploiements avec un alias pondéré

Dans un blue/green déploiement, vous publiez la nouvelle version en même temps que la version actuelle et vous utilisez un alias avec une configuration de routage pour envoyer un pourcentage du trafic vers la nouvelle version. Vous invoquez la fonction via l'ARN qualifié d'alias. Pour avancer le déploiement, vous augmentez le poids de la nouvelle version ; pour l'annuler, vous le reportez à la version précédente.

L'exemple suivant utilise le AWS CLI pour envoyer 10 % du trafic vers la version 2 version complète 1 continue de desservir les 90 % restants.

```
aws lambda update-alias \
  --function-name my-managed-instance-function \
  --name production \
```

```
  --function-version 1 \
  --routing-config AdditionalVersionWeights={"2"=0.1}
```

Dans cette commande :

- `my-managed-instance-function` est le nom de votre fonction.
- `production` est le nom de l'alias que vous invoquez.
- `--function-version 1` est la version qui continue de recevoir le trafic restant.
- `AdditionalVersionWeights={"2"=0.1}` envoie 10 % du trafic à la version 2.

Pour revenir en arrière, effacez la configuration de routage afin que tout le trafic revienne à la version stable.

```
aws lambda update-alias \
  --function-name my-managed-instance-function \
  --name production \
  --function-version 1 \
  --routing-config '{}'
```

Dans cette commande, `--routing-config '{}'` efface la configuration de routage afin que tout le trafic revienne à la version dans `--function-version`, version 1.

Déploiements Canary avec AWS CodeDeploy

Pour automatiser un blue/green changement de trafic, utilisation AWS CodeDeploy. CodeDeploy déplace le trafic de la version actuelle vers la nouvelle version en fonction d'une configuration de déploiement, par exemple en envoyant 10 % du trafic vers la nouvelle version, en attendant cinq minutes, puis en déplaçant le reste. Si un CloudWatch l'alarme associée au déploiement passe en état d'alarme pendant le quart de travail, CodeDeploy annule automatiquement le déploiement.

Pour plus d'informations sur CodeDeploy configurations de déploiement pour Lambda, voir Configurations de déploiement sur une plateforme de calcul Lambda dans le AWS CodeDeploy Guide de l'utilisateur.

Choisir entre $LATEST.PUBLISHED et versions numériques avec alias

Les deux modèles de déploiement introduisent des modifications progressivement. Si vous mettez à jour `$LATEST.PUBLISHED` ou déplacez le trafic à l'aide d'un alias pondéré, Lambda Managed Instances remplace les environnements d'exécution de l'ancienne version par la nouvelle version

par étapes, plutôt que d'un seul coup. Cette approche permet d'utiliser les instances de manière efficace pendant le déploiement. Au lieu de provisionner à l'avance un deuxième ensemble complet d'environnements d'exécution, Lambda les remplace par étapes : à chaque étape, il récupère de la capacité de l'ancienne version avant de lancer le lot suivant de la nouvelle version, de sorte que le déploiement évite d'atteindre le double de la capacité de base.

Comment $LATEST.PUBLISHED progression des déploiements

Lorsque vous publiez une mise à jour de `$LATEST.PUBLISHED`, Lambda commence le déploiement de la nouvelle version par étapes. À chaque étape, Lambda crée de nouveaux environnements d'exécution (jusqu'à 20 % du total de l'ancienne version) et remplace progressivement les environnements d'exécution de l'ancienne version.

Deux facteurs déterminent la durée du déploiement :

- Durée d'initialisation - Chaque étape attend l'initialisation des nouveaux environnements d'exécution avant de poursuivre. Si l'initialisation prend 10 minutes, chaque étape attend au moins 10 minutes.
- Durée d'invocation - Avant que Lambda puisse supprimer un ancien environnement d'exécution, ses appels en cours de vol doivent être terminés (drainés). Si la durée moyenne de votre appel est de 5 minutes, la vidange prend environ 5 minutes en moyenne à chaque étape.

Étant donné que les instances gérées Lambda maintiennent un taux d'utilisation élevé des instances, l'initialisation et la vidange contribuent à la durée totale du déploiement. Les fonctions dont l'initialisation est longue ou les appels de longue durée mettent plus de temps à être complètement déployées.

Comment progressent les versions numériques avec alias

Les mises à jour pondérées des alias sont progressives de la même manière. Lorsque vous modifiez les pondérations de routage sur un alias, par exemple, de 90 % en version 1 et 10 % en version 2 à 100 % en version 2, Lambda Managed Instances remplace lentement les environnements d'exécution de la version 1 par la version 2, sans provisionner de capacité d'instance excédentaire.

Utilisez des versions numériques avec un alias lorsque vous souhaitez contrôler plus étroitement le déploiement progressif et l'observabilité spécifique à la version. Chaque version étant un qualificatif distinct, vous pouvez comparer les statistiques par version pour la version Canary et la version stable avant de promouvoir une modification. Pour plus d'informations, voir affichage des métriques pour vos fonctions Lambda.

Configuration de la mise à l'échelle après un déploiement

Chaque version de fonction que vous déployez possède sa propre configuration de dimensionnement, qui contrôle le nombre minimum et maximum d'environnements d'exécution gérés par Lambda pour cette version. Définissez la configuration de dimensionnement après avoir publié une version afin que la nouvelle version puisse traiter le trafic à la capacité que vous attendez.

L'exemple suivant définit la configuration de dimensionnement pour une version spécifique. Remplacer 2 avec votre numéro de version ou avec `$LATEST.PUBLISHED`.

```
aws lambda put-function-scaling-config \
  --function-name my-managed-instance-function \
  --qualifier 2 \
  --function-scaling-config MinExecutionEnvironments=3,MaxExecutionEnvironments=20
```

Gestion des déploiements à l'aide de l'infrastructure sous forme de code

Vous pouvez définir et déployer les fonctions des instances gérées Lambda et leurs fournisseurs de capacité avec une infrastructure en tant que code, notamment AWS CloudFormation, le AWS Kit de développement cloud (AWS CDK) et des outils tiers tels que HashiCorp Terraforme. Modélisez votre fournisseur de capacité, votre fonction, vos versions et votre alias en tant que ressources afin que votre stratégie de déploiement soit reproductible et révisable.

Gardez les considérations suivantes à l'esprit lorsque vous gérez des déploiements d'instances gérées Lambda avec IaC :

- Publiez une version pour activer une modification. Une nouvelle version de fonction n'est active sur les instances du fournisseur de capacité qu'après sa publication. Modélisez chaque version que vous souhaitez conserver en service, par exemple, les deux côtés d'un blue/green shift, en tant que ressource propre.
- La configuration de mise à l'échelle se fait par version. Appliquez les paramètres d'environnement d'exécution minimum et maximum à chaque version ou à `$LATEST.PUBLISHED`. Si votre outil IaC ne modélise pas directement la configuration de mise à l'échelle, définissez-le à l'aide du `put-function-scaling-config` AWS Commande CLI après le déploiement.
- Les packages de déploiement doivent provenir d'Amazon S3 lorsque vous utilisez AWS API de contrôle du cloud. Le AWS L'API Cloud Control accepte le code d'une fonction uniquement en tant qu'emplacement Amazon S3 ou URI d'image de conteneur, et non en tant que fichier .zip téléchargé localement. Si votre outil IaC utilise cette API, chargez d'abord votre package de

déploiement dans un compartiment S3 et référencez-le par compartiment et clé. Utilisez un bucket versionné afin de détecter les mises à jour de l'objet.

Exemple : CloudFormation modèle

Les suivants CloudFormation le modèle montre un blue/green déploiement. Il crée un fournisseur de capacité, une fonction Lambda Managed Instances, deux versions publiées (chacune avec sa propre configuration de dimensionnement des fonctions) et un alias nommé `production` qui achemine 90 % du trafic vers la version stable et 10 % vers la version Canary. Pour promouvoir le canari, définissez son alias `FunctionVersion` vers la version Canary et supprimez le `RoutingConfig`. Pour revenir en arrière, retirez `RoutingConfig` afin que tout le trafic revienne à la version stable. Remplacez le sous-réseau, le groupe de sécurité, le rôle et les valeurs Amazon S3 par les vôtres.

```
AWSTemplateFormatVersion: '2010-09-09'
Description: Lambda Managed Instances blue/green deployment with a weighted alias

Resources:
  MyCapacityProvider:
    Type: AWS::Lambda::CapacityProvider
    Properties:
      CapacityProviderName: my-capacity-provider
      VpcConfig:
        SubnetIds:
          - subnet-0123456789abcdef0
        SecurityGroupIds:
          - sg-0123456789abcdef0
      PermissionsConfig:
        CapacityProviderOperatorRoleArn: arn:aws:iam::111122223333:role/my-capacity-
provider-operator-role
      InstanceRequirements:
        Architectures:
          - arm64

  MyFunction:
    Type: AWS::Lambda::Function
    Properties:
      FunctionName: my-managed-instance-function
      Role: arn:aws:iam::111122223333:role/my-function-execution-role
      Runtime: python3.13
      Handler: index.lambda_handler
      Architectures:
        - arm64
```

```
      Code:
        S3Bucket: my-deployment-bucket
        S3Key: function.zip
      CapacityProviderConfig:
        LambdaManagedInstancesCapacityProviderConfig:
          CapacityProviderArn: !GetAtt MyCapacityProvider.Arn

  # Stable version - receives the majority of traffic
  StableVersion:
    Type: AWS::Lambda::Version
    Properties:
      FunctionName: !Ref MyFunction
      FunctionScalingConfig:
        MinExecutionEnvironments: 10
        MaxExecutionEnvironments: 50

  # Canary version - receives a small percentage of traffic
  CanaryVersion:
    Type: AWS::Lambda::Version
    Properties:
      FunctionName: !Ref MyFunction
      FunctionScalingConfig:
        MinExecutionEnvironments: 3
        MaxExecutionEnvironments: 20

  ProductionAlias:
    Type: AWS::Lambda::Alias
    Properties:
      FunctionName: !Ref MyFunction
      Name: production
      FunctionVersion: !GetAtt StableVersion.Version
      RoutingConfig:
        AdditionalVersionWeights:
          - FunctionVersion: !GetAtt CanaryVersion.Version
            FunctionWeight: 0.1
```

Exemple : CDK

L'exemple CDK suivant (TypeScript) définit le même fournisseur de capacité et la même fonction en utilisant les constructions de niveau 1 (L1) du `aws-cdk-lib/aws-lambda` module. `operatorRole` et `executionRole` sont des rôles IAM définis ailleurs dans votre stack.

```
import * as cdk from 'aws-cdk-lib';
```

```
import * as lambda from 'aws-cdk-lib/aws-lambda';

const capacityProvider = new lambda.CfnCapacityProvider(this, 'MyCapacityProvider', {
  capacityProviderName: 'my-capacity-provider',
  vpcConfig: {
    subnetIds: ['subnet-0123456789abcdef0'],
    securityGroupIds: ['sg-0123456789abcdef0'],
  },
  permissionsConfig: {
    capacityProviderOperatorRoleArn: operatorRole.roleArn,
  },
  instanceRequirements: {
    architectures: ['arm64'],
  },
});

const fn = new lambda.CfnFunction(this, 'MyFunction', {
  functionName: 'my-managed-instance-function',
  role: executionRole.roleArn,
  runtime: 'python3.13',
  handler: 'index.lambda_handler',
  architectures: ['arm64'],
  code: { s3Bucket: 'my-deployment-bucket', s3Key: 'function.zip' },
  capacityProviderConfig: {
    lambdaManagedInstancesCapacityProviderConfig: {
      capacityProviderArn: capacityProvider.attrArn,
    },
  },
  functionScalingConfig: {
    minExecutionEnvironments: 3,
    maxExecutionEnvironments: 20,
  },
  publishToLatestPublished: true,
});
fn.addDependency(capacityProvider);
```

Exemple : déploiement de Canary avec AWS CodeDeploy

L'exemple CDK suivant (TypeScript) utilisations AWS CodeDeploy pour transférer automatiquement le trafic vers une nouvelle version de fonction. Le `LambdaDeploymentGroup` envoie 10 % du trafic vers la nouvelle version pendant cinq minutes, puis déplace le reste. Si le CloudWatch l'alarme passe en état d'alarme pendant le déploiement, CodeDeploy revient à la version précédente.

`fn` est le L1 `CfnFunction` à partir de l'exemple précédent. Parce que CodeDeploys `LambdaDeploymentGroup` fonctionne avec l'alias de niveau 2 (L2) et les constructions de fonction, importe la fonction L1 par ARN et crée la version et l'alias à partir de celle-ci.

```
import * as cdk from 'aws-cdk-lib';
import * as lambda from 'aws-cdk-lib/aws-lambda';
import * as codedeploy from 'aws-cdk-lib/aws-codedeploy';
import * as cloudwatch from 'aws-cdk-lib/aws-cloudwatch';

// Import the L1 function so that L2 constructs can reference it.
const importedFn = lambda.Function.fromFunctionArn(this, 'ImportedFunction',
 fn.attrArn);

// Publish the version that CodeDeploy shifts traffic to.
const canaryVersion = new lambda.CfnVersion(this, 'CanaryVersion', {
  functionName: fn.ref,
});

// Create the alias that CodeDeploy shifts traffic on.
const alias = new lambda.Alias(this, 'ProductionAlias', {
  aliasName: 'production',
  version: lambda.Version.fromVersionAttributes(this, 'CanaryVersionRef', {
    lambda: importedFn,
    version: canaryVersion.attrVersion,
  }),
});

// Roll back automatically if this alarm fires during the deployment.
const errorAlarm = new cloudwatch.Alarm(this, 'ErrorAlarm', {
  metric: importedFn.metricErrors({ period: cdk.Duration.minutes(1) }),
  threshold: 5,
  evaluationPeriods: 1,
  comparisonOperator: cloudwatch.ComparisonOperator.GREATER_THAN_OR_EQUAL_TO_THRESHOLD,
});

new codedeploy.LambdaDeploymentGroup(this, 'CanaryDeployment', {
  alias,
  deploymentConfig: codedeploy.LambdaDeploymentConfig.CANARY_10PERCENT_5MINUTES,
  alarms: [errorAlarm],
  autoRollback: {
    failedDeployment: true,
    deploymentInAlarm: true,
  },
```

```
});
```

Étapes suivantes

- Comprenez mise à l'échelle pour les instances gérées Lambda
- En savoir plus sur fournisseurs de capacité pour les instances gérées Lambda
- Révision meilleures pratiques pour les instances gérées Lambda

Exécutions des instances gérées Lambda

Les fonctions d'événements Lambda sur les instances gérées Lambda prennent en charge les deux `.zip` des packages de déploiement d'archives de fichiers et d'images de conteneurs, qui utilisent le format Open Container Initiative (OCI). Pour réduire le temps de démarrage des images de conteneurs de grande taille, voir Lazy-load images de conteneurs avec Seekable OCI (SOCI).

Lambda traite les demandes différemment lorsqu'il utilise des instances gérées Lambda. Au lieu de gérer les demandes de manière séquentielle dans chaque environnement d'exécution, les instances gérées Lambda traitent plusieurs demandes simultanément dans chaque environnement d'exécution. Cette modification du modèle d'exécution signifie que les fonctions événementielles Lambda utilisant des instances gérées Lambda doivent prendre en compte la sécurité des threads, la gestion des états et l'isolation du contexte. Ces problèmes ne se posent pas dans le modèle de concurrence unique Lambda (par défaut). De plus, l'implémentation multi-simultanéité varie selon les environnements d'exécution.

Langues prises en charge

Les instances gérées Lambda peuvent être utilisées avec les langages de programmation et les environnements d'exécution suivants :

- Java : Java 21 et versions ultérieures.
- Python : Python 3.13 et versions ultérieures.
- Node.js: Node.js 22 et versions ultérieures.
- .NET : .NET 8 et versions ultérieures.
- Rouille : Supporté à l'aide du OS-only exécution `provided.al2023` et plus tard.

Language-specific considérations

Chaque langage de programmation implémente différemment la multiconcurrence. Vous devez comprendre comment la multiconcurrence est implémentée dans le langage de programmation que vous avez choisi pour appliquer les meilleures pratiques de simultanéité appropriées.

Java

Utilise un processus unique avec des threads du système d'exploitation pour la simultanéité. Plusieurs threads exécutent la méthode du gestionnaire simultanément, ce qui nécessite une gestion sûre de l'état et des ressources partagées.

Python

Utilise plusieurs processus Python dans lesquels chaque demande simultanée est exécutée dans un processus distinct. Cela protège contre la plupart des problèmes de simultanéité, bien qu'il faille faire attention aux ressources partagées telles que `/tmp` annuaire.

Node.js

Utilisations fils de discussion pour travailleurs avec exécution asynchrone. Les demandes simultanées sont réparties entre les threads de travail, et chaque thread de travail peut également gérer les demandes simultanées de manière asynchrone, ce qui nécessite une gestion sécurisée de l'état et des ressources partagées.

.NET

Utilise les tâches .NET avec le traitement asynchrone de plusieurs demandes simultanées. Nécessite une gestion sûre de l'État et des ressources partagées.

Rust

Utilise un processus unique avec des tâches asynchrones alimentées par Tokyo. Le gestionnaire doit être `Clone` + `Send`.

Étapes suivantes

Pour obtenir des informations détaillées sur chaque environnement d'exécution, consultez les rubriques suivantes :

- Runtime Java pour les instances gérées Lambda
- Node.js runtime pour les instances gérées Lambda

- Runtime Python pour les instances gérées Lambda
- Runtime .NET pour les instances gérées Lambda
- Support Rust pour les instances gérées Lambda

Runtime Java pour les instances gérées Lambda

Pour les environnements d'exécution Java, les instances gérées Lambda utilisent des threads du système d'exploitation pour la simultanéité. Lambda charge votre objet gestionnaire une fois par environnement d'exécution lors de l'initialisation, puis crée plusieurs threads. Ces threads s'exécutent en parallèle et nécessitent une gestion sûre de l'état et des ressources partagées. Chaque thread partage le même objet gestionnaire et tous les champs statiques.

Configuration de la simultanéité

Le nombre maximum de requêtes simultanées que Lambda envoie à chaque environnement d'exécution est contrôlé par le `PerExecutionEnvironmentMaxConcurrency` paramètre de la configuration de la fonction. Il s'agit d'un paramètre facultatif et la valeur par défaut varie en fonction de l'exécution. Pour les environnements d'exécution Java, la valeur par défaut est de 32 requêtes simultanées par processeur virtuel, ou vous pouvez configurer votre propre valeur. Cette valeur détermine également le nombre de threads utilisés par le moteur d'exécution Java. Lambda ajuste automatiquement le nombre de demandes simultanées jusqu'au maximum configuré en fonction de la capacité de chaque environnement d'exécution à absorber ces demandes.

Création de fonctions pour la multisimultanéité

Vous devez appliquer les mêmes pratiques de sécurité des threads lorsque vous utilisez des instances gérées Lambda que dans tout autre environnement multithread. Étant donné que l'objet du gestionnaire est partagé entre tous les threads de travail d'exécution, tout état mutable doit être sûr pour les threads. Cela inclut les collections, les connexions aux bases de données et tous les objets statiques modifiés lors du traitement des demandes.

AWS Les clients du SDK sont sûrs pour les threads et ne nécessitent aucune manipulation particulière.

Exemple : pools de connexions à la base de données

Le code suivant utilise un objet de connexion à une base de données statique qui est partagé entre les threads. Selon la bibliothèque de connexion utilisée, cela peut ne pas être compatible avec les threads.

```
public class DBQueryHandler implements RequestHandler<Object, String> {
    // Single connection shared across all threads - NOT SAFE
    private static Connection connection;

    public DBQueryHandler() {
        this.connection = DriverManager.getConnection(jdbcUrl, username, password);
    }

    @Override
    public String handleRequest(Object input, Context context) {
        PreparedStatement stmt = connection.prepareStatement(query);
        ResultSet rs = stmt.executeQuery();
        // Multiple threads using same connection causes issues
        return result.toString();
    }
}
```

Une approche sûre des threads consiste à utiliser un pool de connexions. Dans l'exemple suivant, le gestionnaire de fonctions récupère une connexion depuis le pool. La connexion n'est utilisée que dans le cadre d'une seule demande.

```
public class DBQueryHandler implements RequestHandler<Object, String> {

    private static HikariDataSource dataSource;

    public DBQueryHandler() {
        HikariConfig config = new HikariConfig();
        config.setJdbcUrl("jdbc:mysql://localhost:3306/your_database");
        dataSource = new HikariDataSource(config); // Create pool once per Lambda
 container
    }

    @Override
    public String handleRequest(Object input, Context context) {
        String query = "SELECT column_name FROM your_table LIMIT 10";
        StringBuilder result = new StringBuilder("Data:\n");

        // try-with-resources automatically calls close() on the connection,
        // which returns it to the HikariCP pool (does NOT close the physical DB
 connection)
        try (Connection connection = dataSource.getConnection();
             PreparedStatement stmt = connection.prepareStatement(query);
```

```
             ResultSet rs = stmt.executeQuery()) {

            while (rs.next()) {
                result.append(rs.getString("column_name")).append("\n");
            }

        } catch (Exception e) {
            context.getLogger().log("Error: " + e.getMessage());
            return "Error";
        }

        return result.toString();
    }
}
```

Exemple : Collections

Les collections Java standard ne sont pas sûres pour les threads :

```
public class Handler implements RequestHandler<Object, String> {
    private static List<String> items = new ArrayList<>();
    private static Map<String, Object> cache = new HashMap<>();

    @Override
    public String handleRequest(Object input, Context context) {
        items.add("list item");  // Not thread-safe
        cache.put("key", input); // Not thread-safe
        return "Success";
    }
}
```

Utilisez plutôt des collections adaptées aux threads :

```
public class Handler implements RequestHandler<Object, String> {
    private static final List<String> items =
        Collections.synchronizedList(new ArrayList<>());
    private static final ConcurrentHashMap<String, Object> cache =
        new ConcurrentHashMap<>();

    @Override
    public String handleRequest(Object input, Context context) {
        items.add("list item");  // Thread-safe
        cache.put("key", input); // Thread-safe
```

```
        return "Success";
    }
}
```

Répertoire /tmp partagé

Le `/tmp` répertoire est partagé entre toutes les demandes simultanées de l'environnement d'exécution. Les écritures simultanées dans le même fichier peuvent entraîner une corruption des données, par exemple si un autre processus remplace le fichier. Pour résoudre ce problème, implémentez le verrouillage des fichiers partagés ou utilisez des noms de fichiers uniques par thread ou par requête pour éviter les conflits. N'oubliez pas de nettoyer les fichiers inutiles pour ne pas épuiser l'espace disponible.

Logging

L'entrelacement des journaux (les entrées de journal provenant de différentes demandes sont entrelacées dans les journaux) est normal dans les systèmes multisimultanés.

Les fonctions utilisant des instances gérées Lambda utilisent toujours le format de journal JSON structuré introduit avec les contrôles de journalisation avancés. Ce format inclut le`requestId`, permettant de corréler les entrées du journal à une seule demande. Lorsque vous utilisez l'`LambdaLogger`objet de`context.getLogger()`, `requestId` il est automatiquement inclus dans chaque entrée du journal. Pour plus d'informations, voirthe section called “Utilisation des contrôles de journalisation avancés de Lambda avec Java”.

Contexte de la requête

L'`context`objet est lié au thread de requête. Using `context.getAwsRequestId()` fournit un accès sécurisé à l'ID de demande pour la demande en cours.

Utilisez-le `context.getXrayTraceId()` pour accéder à l'ID de X-Ray trace. Cela fournit un accès sécurisé à l'ID de trace de la demande en cours. Lambda ne prend pas en charge la variable d'`_X_AMZN_TRACE_ID`environnement avec les instances gérées Lambda. L'ID de X-Ray trace est automatiquement propagé lors de l'utilisation du AWS SDK.

Utilisez-le `com.amazonaws.services.lambda.runtime.Context.getRemainingTimeInMillis()` pour détecter les délais d'attente. Pour plus d’informations, consultez the section called “Gestion des erreurs et restauration”.

Si vous utilisez des fils virtuels dans votre programme ou si vous créez des fils lors de l'initialisation, vous devez transmettre tout contexte de demande requis à ces fils.

Exemple : gestion des délais

Vérifiez le temps restant avant chaque unité de travail et arrêtez le traitement avant le déclenchement du timeout. Configurez en BUFFER_MS fonction de la durée prévue de votre prochaine partie de travail.

```
private static final int BUFFER_MS = 2000; // Configure based on your next chunk of
 work

public Map<String, Object> handleRequest(Map<String, Object> event, Context context) {
    for (Object item : (List<Object>) event.get("items")) {
        if (context.getRemainingTimeInMillis() < BUFFER_MS)
            return Map.of("statusCode", 206, "body", "Timeout approaching, stopping
 early");
        processItem(item);
    }
    return Map.of("statusCode", 200, "body", "Done");
}
```

Exemple : Propagation des délais aux appels en aval

Lorsque vous passez des appels vers des services en aval, répartissez le temps restant sous forme de délai d'attente pour éviter de vous accrocher à des appels réseau qui dureraient plus longtemps que votre appel. Utilisez un remplacement par demande sur un client partagé plutôt que de créer un nouveau client par appel :

```
import software.amazon.awssdk.services.s3.S3Client;
import software.amazon.awssdk.services.s3.model.GetObjectRequest;
import java.time.Duration;

private static final S3Client s3 = S3Client.create();

public String handleRequest(Map<String, Object> event, Context context) {
    Duration timeout = Duration.ofMillis(Math.max(1000,
 context.getRemainingTimeInMillis() - 500));

    GetObjectRequest req = GetObjectRequest.builder()
        .bucket("my-bucket").key("my-key")
        .overrideConfiguration(cfg -> cfg.apiCallTimeout(timeout))
```

```
        .build();
    s3.getObject(req);
    return "Done";
}
```

Initialisation et arrêt

L'initialisation des fonctions se produit une fois par environnement d'exécution. Les objets créés lors de l'initialisation sont partagés entre les threads.

Pour les fonctions Lambda dotées d'extensions, l'environnement d'exécution émet un signal SIGTERM lors de l'arrêt. Ce signal est utilisé par les extensions pour déclencher des tâches de nettoyage, telles que le vidage des buffers. Vous pouvez vous abonner aux événements SIGTERM pour déclencher des tâches de nettoyage des fonctions, telles que la fermeture des connexions à la base de données. Pour en savoir plus sur le cycle de vie de l'environnement d'exécution, veuillez consulter the section called “Environnement d’exécution”.

Versions de dépendance

Les instances gérées Lambda nécessitent les versions de package minimales suivantes :

- AWS SDK pour Java 2.0 : version 2.34.0 ou ultérieure
- AWS X-Ray SDK pour Java : version 2.20.0 ou ultérieure
- AWS Distribution pour OpenTelemetry - Instrumentation pour Java : version 2.20.0 ou ultérieure
- Powertools pour AWS Lambda (Java) : version 2.8.0 ou ultérieure

Outils électriques pour AWS Lambda (Java)

Powertools for AWS Lambda (Java) est compatible avec les instances gérées Lambda et fournit des utilitaires pour la journalisation, le suivi, les métriques, etc. Pour plus d'informations, consultez Powertools for AWS Lambda (Java).

Étapes suivantes

- Vérifier le Node.js temps d'exécution pour les instances gérées Lambda
- Vérifier l'environnement d'exécution Python pour les instances gérées Lambda
- Vérifier l'environnement d'exécution .NET pour les instances gérées Lambda
- En savoir plus sur la mise à l'échelle des instances gérées Lambda

Node.js environnement d'exécution pour les instances gérées Lambda

Pour les Node.js environnements d'exécution, les instances gérées Lambda utilisent des threads de travail avec une exécution `await` basée sur`async`/pour gérer les demandes simultanées. L'initialisation de la fonction se produit une fois par thread de travail. Les appels simultanés sont gérés selon deux dimensions : les threads de travail fournissent le parallélisme entre les vCPU et l'exécution asynchrone assure la simultanéité au sein de chaque thread. Chaque demande simultanée gérée par le même thread de travail partage le même objet de gestionnaire et le même état global, ce qui nécessite une gestion sécurisée lors de plusieurs demandes simultanées.

Simultanéité maximum

Le nombre maximum de requêtes simultanées que Lambda envoie à chaque environnement d'exécution est contrôlé par le `PerExecutionEnvironmentMaxConcurrency` paramètre de la configuration de la fonction. Il s'agit d'un paramètre facultatif et la valeur par défaut varie en fonction de l'exécution. Pour les Node.js environnements d'exécution, la valeur par défaut est de 64 requêtes simultanées par processeur virtuel, ou vous pouvez configurer votre propre valeur. Lambda ajuste automatiquement le nombre de demandes simultanées jusqu'au maximum configuré en fonction de la capacité de chaque environnement d'exécution à absorber ces demandes.

En Node.js effet, le nombre de requêtes simultanées que chaque environnement d'exécution peut traiter est déterminé par le nombre de threads de travail et la capacité de chaque thread de travail à traiter les demandes simultanées de manière asynchrone. Le nombre par défaut de threads de travail est déterminé par le nombre de vCPU disponibles, ou vous pouvez configurer le nombre de threads de travail en définissant la variable d'`AWS_LAMBDA_NODEJS_WORKER_COUNT`environnement. Nous vous recommandons d'utiliser des gestionnaires de fonctions asynchrones car cela permet de traiter plusieurs demandes par thread de travail. Si votre gestionnaire de fonctions est synchrone, chaque thread de travail ne peut traiter qu'une seule demande à la fois.

Création de fonctions pour la multisimultanéité

Avec un gestionnaire de fonctions asynchrone, chaque worker d'exécution traite plusieurs demandes simultanément. Les objets globaux sont partagés entre plusieurs demandes simultanées. Pour les objets mutables, évitez d'utiliser l'état global ou l'utilisation`AsyncLocalStorage`.

AWS Les clients du SDK sont asynchrones et ne nécessitent aucune manipulation particulière.

Exemple : État global

Le code suivant utilise un objet global qui est muté dans le gestionnaire de fonctions. Ce n'est pas sécurisé pour l'asynchronisation.

```
let state = {
    currentUser: null,
    requestData: null
};

export const handler = async (event, context) => {
    state.currentUser = event.userId;
    state.requestData = event.data;

    await processData(state.requestData);

    // state.currentUser might now belong to a different request
    return { user: state.currentUser };
};
```

L'initialisation de l'`state`objet dans le gestionnaire de fonctions permet d'éviter le partage de l'état global.

```
export const handler = async (event, context) => {
    let state = {
        currentUser: event.userId,
        requestData: event.data
    };

    await processData(state.requestData);

    return { user: state.currentUser };
};
```

Exemple : connexions à une base de données

Le code suivant utilise un objet client partagé qui est partagé entre plusieurs invocations. Selon la bibliothèque de connexion utilisée, cela peut ne pas être sécurisé en matière de simultanéité.

```
const { Client } = require('pg');

// Single connection created at init time
const client = new Client({
  host: process.env.DB_HOST,
```

```
  database: process.env.DB_NAME,
  user: process.env.DB_USER,
  password: process.env.DB_PASSWORD
});

// Connect once during cold start
client.connect();

exports.handler = async (event) => {
  // Multiple parallel invocations share this single connection = BAD
  // With multi-concurrent Lambda, queries will collide
  const result = await client.query('SELECT * FROM users WHERE id = $1',
 [event.userId]);

  return {
    statusCode: 200,
    body: JSON.stringify(result.rows[0])
  };
};
```

Une approche sûre en matière de concurrence consiste à utiliser un pool de connexions. Le pool utilise une connexion distincte pour chaque requête de base de données simultanée.

```
const { Pool } = require('pg');

// Connection pool created at init time
const pool = new Pool({
  host: process.env.DB_HOST,
  database: process.env.DB_NAME,
  user: process.env.DB_USER,
  password: process.env.DB_PASSWORD,
  max: 20,  // Max connections in pool
  idleTimeoutMillis: 30000,
  connectionTimeoutMillis: 2000
});

exports.handler = async (event) => {
  // Pool gives each parallel invocation its own connection
  const result = await pool.query('SELECT * FROM users WHERE id = $1', [event.userId]);

  return {
    statusCode: 200,
    body: JSON.stringify(result.rows[0])
```

```
  };
};
```

Node.js 22 gestionnaires basés sur les rappels

Lorsque vous utilisez Node.js 22, vous ne pouvez pas utiliser de gestionnaire de fonctions basé sur des rappels avec les instances gérées Lambda. Callback-based les gestionnaires ne sont pris en charge que pour les fonctions Lambda (par défaut). Pour les versions Node.js 24 et ultérieures, les gestionnaires de fonctions basés sur les rappels sont obsolètes pour les instances Lambda (par défaut) et Lambda Managed Instances.

Utilisez plutôt un gestionnaire de `async` fonctions lorsque vous utilisez des instances gérées Lambda. Pour plus d'informations, voir Définir le gestionnaire de fonctions Lambda dans. Node.js

Répertoire /tmp partagé

Le `/tmp` répertoire est partagé entre toutes les demandes simultanées de l'environnement d'exécution. Les écritures simultanées dans le même fichier peuvent entraîner une corruption des données, par exemple si un autre processus remplace le fichier. Pour résoudre ce problème, implémentez le verrouillage des fichiers partagés ou utilisez des noms de fichiers uniques par demande pour éviter les conflits. N'oubliez pas de nettoyer les fichiers inutiles pour ne pas épuiser l'espace disponible.

Logging

L'entrelacement des journaux (les entrées de journal provenant de différentes demandes sont entrelacées dans les journaux) est normal dans les systèmes multisimultanés. Les fonctions utilisant des instances gérées Lambda utilisent toujours le format de journal JSON structuré introduit avec les contrôles de journalisation avancés. Ce format inclut le`requestId`, permettant de corréler les entrées du journal à une seule demande. Lorsque vous utilisez l'`console`enregistreur, il `requestId` est automatiquement inclus dans chaque entrée du journal. Pour plus d'informations, voirthe section called “Utilisation des commandes de journalisation avancées de Lambda avec Node.js”.

Les bibliothèques de journalisation tierces les plus populaires, telles que Winston, incluent généralement la prise en charge de l'utilisation de la console pour la sortie des journaux.

Contexte de la requête

Using `context.awsRequestId` fournit un accès asynchrone sécurisé à l'ID de demande pour la demande en cours.

Utilisez-le `context.xRayTraceId` pour accéder à l'ID de X-Ray trace. Cela fournit un accès sécurisé en cas de concurrence à l'ID de trace de la demande en cours. Lambda ne prend pas en charge la variable d'`_X_AMZN_TRACE_ID`environnement avec les instances gérées Lambda. L'ID de X-Ray trace est automatiquement propagé lors de l'utilisation du AWS SDK.

Utilisez-le `context.getRemainingTimeInMillis()` pour détecter les délais d'attente. Pour plus d'informations, consultez the section called “Gestion des erreurs et restauration”.

Exemple : gestion des délais

Vérifiez le temps restant avant chaque unité de travail et arrêtez le traitement avant le déclenchement du timeout. Configurez en `BUFFER_MS` fonction de la durée prévue de votre prochaine partie de travail.

```
const BUFFER_MS = 2000; // Configure based on your next chunk of work

exports.handler = async (event, context) => {
    for (const item of event.items) {
        if (context.getRemainingTimeInMillis() < BUFFER_MS)
            return { statusCode: 206, body: "Timeout approaching, stopping early" };
        await processItem(item);
    }
    return { statusCode: 200, body: "Done" };
};
```

Exemple : Propagation des délais aux appels en aval

Lorsque vous passez des appels vers des services en aval, répartissez le temps restant sous forme de délai d'attente pour éviter de vous accrocher à des appels réseau qui dureraient plus longtemps que votre appel :

```
const { S3Client, GetObjectCommand } = require("@aws-sdk/client-s3");
const client = new S3Client({});

exports.handler = async (event, context) => {
    const timeout = Math.max(1000, context.getRemainingTimeInMillis() - 500);
    const response = await client.send(
        new GetObjectCommand({ Bucket: "my-bucket", Key: "my-key" }),
        { abortSignal: AbortSignal.timeout(timeout) }
    );
    return { statusCode: 200, body: "Done" };
```

```
};
```

Initialisation et arrêt

L'initialisation de la fonction se produit une fois par thread de travail. Il est possible que des entrées de journal se répètent si votre fonction émet des journaux lors de l'initialisation.

Pour les fonctions Lambda dotées d'extensions, l'environnement d'exécution émet un signal SIGTERM lors de l'arrêt. Ce signal est utilisé par les extensions pour déclencher des tâches de nettoyage, telles que le vidage des buffers. Les fonctions Lambda (par défaut) avec des extensions peuvent également s'abonner au signal SIGTERM en utilisant. `process.on()` Ceci n'est pas pris en charge pour les fonctions utilisant des instances gérées Lambda car il `process.on()` ne peut pas être utilisé avec des threads de travail. Pour en savoir plus sur le cycle de vie de l'environnement d'exécution, veuillez consulter the section called “Environnement d’exécution”.

Versions de dépendance

Les instances gérées Lambda nécessitent les versions de package minimales suivantes :

- AWS SDK pour JavaScript v3 : version 3.933.0 ou ultérieure
- AWS X-Ray SDK pour Node.js : version 3.12.0 ou ultérieure
- AWS Distribution pour OpenTelemetry - Instrumentation pour JavaScript : version 0.8.0 ou ultérieure
- Powertools pour AWS Lambda (TypeScript) : version 2.29.0 ou ultérieure

Outils électriques pour AWS Lambda () TypeScript

Powertools for AWS Lambda (TypeScript) est compatible avec les instances gérées Lambda et fournit des utilitaires pour la journalisation, le suivi, les métriques, etc. Pour plus d'informations, consultez Powertools for AWS Lambda ()TypeScript.

Étapes suivantes

- Consulter le moteur d'exécution Java pour les instances gérées Lambda
- Vérifier l'environnement d'exécution Python pour les instances gérées Lambda
- Vérifier l'environnement d'exécution .NET pour les instances gérées Lambda
- En savoir plus sur la mise à l'échelle des instances gérées Lambda

Runtime Python pour les instances gérées Lambda

L'environnement d'exécution Lambda utilise plusieurs processus Python pour gérer les demandes simultanées. Chaque demande simultanée s'exécute dans un processus distinct avec son propre espace mémoire et son propre initialisation. Chaque processus traite une demande à la fois, de manière synchrone. Les processus ne partageant pas directement la mémoire, les variables globales, les caches au niveau des modules et les objets singleton sont isolés entre les requêtes simultanées.

Configuration de la simultanéité

Le nombre maximum de requêtes simultanées que Lambda envoie à chaque environnement d'exécution est contrôlé par le `PerExecutionEnvironmentMaxConcurrency` paramètre de la configuration de la fonction. Il s'agit d'un paramètre facultatif et la valeur par défaut varie en fonction de l'exécution. Pour les environnements d'exécution Python, la valeur par défaut est de 16 requêtes simultanées par processeur virtuel, ou vous pouvez configurer votre propre valeur. Cette valeur détermine également le nombre de processus utilisés par le moteur d'exécution Python. Lambda ajuste automatiquement le nombre de demandes simultanées jusqu'au maximum configuré en fonction de la capacité de chaque environnement d'exécution à absorber ces demandes.

> **Important**
>
> L'utilisation de la simultanéité basée sur les processus signifie que chaque processus de travail d'exécution effectue sa propre initialisation. L'utilisation totale de la mémoire est égale à la mémoire par processus multipliée par le nombre de processus simultanés. Si vous chargez des bibliothèques ou des ensembles de données volumineux et que vous avez une simultanéité élevée, votre empreinte mémoire est importante. En fonction de votre charge de travail, vous devrez peut-être ajuster votre CPU-to-memory ratio ou utiliser un paramètre de simultanéité inférieur pour éviter de dépasser la mémoire disponible. Vous pouvez utiliser la `MemoryUtilization` métrique CloudWatch pour suivre la consommation de mémoire.

Création de fonctions pour la multisimultanéité

En raison du modèle multi-simultanéité basé sur les processus, les fonctions Lambda Managed Instances utilisant des environnements d'exécution Python n'accèdent pas aux ressources en mémoire simultanément à partir de plusieurs appels. Il n'est pas nécessaire d'appliquer des pratiques de codage pour garantir la sécurité de la simultanéité en mémoire.

Répertoire /tmp partagé

Le `/tmp` répertoire est partagé entre toutes les demandes simultanées de l'environnement d'exécution. Les écritures simultanées dans le même fichier peuvent entraîner une corruption des données, par exemple si un autre processus remplace le fichier. Pour résoudre ce problème, implémentez le verrouillage des fichiers partagés ou utilisez des noms de fichiers uniques par processus ou par demande pour éviter les conflits. N'oubliez pas de nettoyer les fichiers inutiles pour ne pas épuiser l'espace disponible.

Logging

L'entrelacement des journaux (les entrées de journal provenant de différentes demandes sont entrelacées dans les journaux) est normal dans les systèmes multisimultanés.

Les fonctions utilisant des instances gérées Lambda utilisent toujours le format de journal JSON structuré introduit avec les contrôles de journalisation avancés. Ce format inclut le`requestId`, permettant de corréler les entrées du journal à une seule demande. Lorsque vous utilisez le `logging` module de la bibliothèque standard Python dans Lambda, `requestId` il est automatiquement inclus dans chaque entrée de journal. Pour plus d'informations, consultez la section Utilisation des contrôles de journalisation avancés Lambda avec Python.

Contexte de la requête

`context.aws_request_id`Utilisez-le pour accéder à l'ID de demande pour la demande en cours.

Avec les environnements d'exécution Python, vous pouvez utiliser la variable d'`_X_AMZN_TRACE_ID`environnement pour accéder à l'ID de X-Ray trace avec les instances gérées Lambda. L'ID de X-Ray trace est automatiquement propagé lors de l'utilisation du AWS SDK.

Utilisez-le `context.get_remaining_time_in_millis()` pour détecter les délais d'attente. Pour plus d'informations, consultez the section called “Gestion des erreurs et restauration”.

Exemple : gestion des délais

Vérifiez le temps restant avant chaque unité de travail et arrêtez le traitement avant le déclenchement du timeout. Configurez en `BUFFER_MS` fonction de la durée prévue de votre prochaine partie de travail.

```
BUFFER_MS = 2000  # Configure based on your next chunk of work

def handler(event, context):
    for item in event["items"]:
```

```
        if context.get_remaining_time_in_millis() < BUFFER_MS:
            return {"statusCode": 206, "body": "Timeout approaching, stopping early"}
        process_item(item)
    return {"statusCode": 200, "body": "Done"}
```

Exemple : Propagation des délais aux appels en aval

Lorsque vous passez des appels vers des services en aval, répartissez le temps restant sous forme de délai d'attente pour éviter de vous accrocher à des appels réseau qui dureraient plus longtemps que votre appel. Le SDK boto3 ne prend pas en charge les délais d'expiration par demande sur un client existant. Vous devez donc créer un client avec le délai d'expiration souhaité. Pour les fonctions haut débit, déterminez si un délai d'attente fixe configuré lors de l'initialisation est plus approprié que la création d'un client par demande.

```
import boto3
from botocore.config import Config

def handler(event, context):
    remaining = context.get_remaining_time_in_millis() / 1000
    timeout = max(1, remaining - 0.5)
    s3 = boto3.client("s3", config=Config(read_timeout=timeout,
 connect_timeout=timeout))
    response = s3.get_object(Bucket="my-bucket", Key="my-key")
    return {"statusCode": 200, "body": "Done"}
```

Initialisation et arrêt

L'initialisation de la fonction se produit une fois par processus. Vous pouvez voir des entrées de journal répétées si votre fonction émet des journaux lors de l'initialisation.

Pour les fonctions Lambda dotées d'extensions, l'environnement d'exécution émet un signal SIGTERM lors de l'arrêt. Ce signal est utilisé par les extensions pour déclencher des tâches de nettoyage, telles que le vidage des buffers. Vous pouvez vous abonner aux événements SIGTERM pour déclencher des tâches de nettoyage des fonctions, telles que la fermeture des connexions à la base de données. Pour en savoir plus sur le cycle de vie de l'environnement d'exécution, veuillez consulter the section called “Environnement d’exécution”.

Versions de dépendance

Les instances gérées Lambda nécessitent les versions de package minimales suivantes :

- Powertools pour AWS Lambda (Python) : version 3.23.0 ou ultérieure

Outils électriques pour AWS Lambda (Python)

Powertools for AWS Lambda (Python) est compatible avec les instances gérées Lambda et fournit des utilitaires pour la journalisation, le suivi, les métriques, etc. Pour plus d'informations, consultez Powertools for AWS Lambda (Python).

Étapes suivantes

- Consulter le moteur d'exécution Java pour les instances gérées Lambda
- Vérifier le Node.js temps d'exécution pour les instances gérées Lambda
- Vérifier l'environnement d'exécution .NET pour les instances gérées Lambda
- En savoir plus sur la mise à l'échelle des instances gérées Lambda

Environnement d'exécution .NET pour les instances gérées Lambda

Pour les environnements d'exécution .NET, les instances gérées Lambda utilisent un seul processus .NET par environnement d'exécution. Plusieurs demandes simultanées sont traitées à l'aide de tâches .NET.

Configuration de la simultanéité

Le nombre maximum de demandes simultanées que Lambda envoie à chaque environnement d'exécution est contrôlé par le `PerExecutionEnvironmentMaxConcurrency` paramètre de configuration de la fonction. Il s'agit d'un paramètre facultatif, et la valeur par défaut varie en fonction du temps d'exécution. Pour les environnements d'exécution .NET, la valeur par défaut est de 32 requêtes simultanées par vCPU, ou vous pouvez configurer votre propre valeur. Lambda ajuste automatiquement le nombre de demandes simultanées jusqu'au maximum configuré en fonction de la capacité de chaque environnement d'exécution à absorber ces demandes.

Création de fonctions pour la multisimultanéité

Lorsque vous utilisez des instances gérées Lambda, vous devez appliquer les mêmes pratiques de sécurité en matière de simultanéité que dans tout autre environnement multiconcurrent. Étant donné que l'objet du gestionnaire est partagé entre toutes les tâches, tout état mutable doit être adapté aux threads. Cela inclut les collections, les connexions aux bases de données et tous les objets statiques modifiés lors du traitement des demandes.

AWS Les clients du SDK sont compatibles avec les threads et ne nécessitent aucune manipulation particulière.

Exemple : pools de connexions aux bases de données

Le code suivant utilise un objet de connexion à une base de données statique qui est partagé entre des demandes simultanées. L'`SqlConnection`objet n'est pas compatible avec les threads.

```
public class DBQueryHandler
{
    // Single connection shared across threads - NOT SAFE
    private SqlConnection connection;

    public DBQueryHandler()
    {
        connection = new SqlConnection("your-connection-string-here");
        connection.Open();
    }

    public string Handle(object input, ILambdaContext context)
    {
        using var cmd = connection.CreateCommand();
        cmd.CommandText = "SELECT ..."; // your query

        using var reader = cmd.ExecuteReader();

        ...
    }
}
```

Pour résoudre ce problème, utilisez une connexion distincte pour chaque demande, issue d'un pool de connexions. ADO.NET les fournisseurs tels que le pool de connexions prennent `Microsoft.Data.SqlClient` automatiquement en charge le regroupement de connexions lorsque l'objet de connexion est ouvert.

```
public class DBQueryHandler
{
    public DBQueryHandler()
    {
    }

    public string Handle(object input, ILambdaContext context)
    {
        using var connection = new SqlConnection("your-connection-string-here");
        connection.Open();
```

```
        using var cmd = connection.CreateCommand();
        cmd.CommandText = "SELECT ..."; // your query

        using var reader = cmd.ExecuteReader();

        ...
    }
}
```

Exemple : Collections

Les collections .NET standard ne sont pas adaptées aux threads :

```
public class Handler
{
    private static List<string> items = new List<string>();
    private static Dictionary<string, object> cache = new Dictionary<string, object>();

    public string FunctionHandler(object input, ILambdaContext context)
    {
        items.Add(context.AwsRequestId);
        cache["key"] = input;

        return "Success";
    }
}
```

Utilisez les collections de l'espace de `System.Collections.Concurrent` noms pour des raisons de sécurité en matière de concurrence :

```
public class Handler
{
    private static ConcurrentBag<string> items = new ConcurrentBag<string>();
    private static ConcurrentDictionary<string, object> cache = new
 ConcurrentDictionary<string, object>();

    public string FunctionHandler(object input, ILambdaContext context)
    {
        items.Add(context.AwsRequestId);
        cache["key"] = input;

        return "Success";
    }
```

```
}
```

Répertoire /tmp partagé

Le `/tmp` répertoire est partagé entre toutes les demandes simultanées dans l'environnement d'exécution. Les écritures simultanées dans le même fichier peuvent entraîner une corruption des données, par exemple si une autre demande remplace le fichier. Pour résoudre ce problème, implémentez le verrouillage des fichiers partagés ou utilisez des noms de fichiers uniques par demande afin d'éviter les conflits. N'oubliez pas de nettoyer les fichiers inutiles pour ne pas épuiser l'espace disponible.

Logging

L'entrelacement des journaux (les entrées des journaux provenant de différentes demandes sont entrelacées dans des journaux) est normal dans les systèmes multiconcurrents. Les fonctions utilisant des instances gérées Lambda utilisent toujours le format de journal JSON structuré introduit avec les contrôles de journalisation avancés. Ce format inclut le`requestId`, ce qui permet de corréler les entrées du journal à une seule demande. Lorsque vous utilisez l'`context.Logger`objet pour générer des journaux, ceux-ci `requestId` sont automatiquement inclus dans chaque entrée de journal. Pour de plus amples informations, voirthe section called “Utilisation des contrôles de journalisation avancés de Lambda avec .NET”.

Contexte de la requête

Utilisez la `context.AwsRequestId` propriété pour accéder à l'ID de demande pour la demande en cours.

Utilisez la `context.TraceId` propriété pour accéder à l'ID de X-Ray trace. Cela fournit un accès simultané à l'ID de trace pour la demande en cours. Lambda ne prend pas en charge la variable d'`_X_AMZN_TRACE_ID`environnement avec les instances gérées par Lambda. L'ID de X-Ray trace est propagé automatiquement lors de l'utilisation du AWS SDK.

`ILambdaContext.RemainingTime`À utiliser pour détecter les délais d'expiration. Pour plus d’informations, consultez the section called “Gestion des erreurs et restauration”.

Exemple : gestion des délais

Vérifiez le temps restant avant chaque unité de travail et arrêtez le traitement avant que le délai d'expiration ne se déclenche. Configurez la mémoire tampon en fonction de la durée prévue de votre prochaine tâche.

```
private static readonly TimeSpan Buffer = TimeSpan.FromMilliseconds(2000);

public APIGatewayProxyResponse FunctionHandler(APIGatewayProxyRequest request,
 ILambdaContext context)
{
    var items = JsonSerializer.Deserialize<List<string>>(request.Body);
    foreach (var item in items)
    {
        if (context.RemainingTime < Buffer)
            return new APIGatewayProxyResponse { StatusCode = 206, Body = "Timeout
 approaching, stopping early" };
        ProcessItem(item);
    }
    return new APIGatewayProxyResponse { StatusCode = 200, Body = "Done" };
}
```

Exemple : propagation des délais aux appels en aval

Lorsque vous appelez des services en aval, répartissez le temps restant sous forme de délai d'expiration afin d'éviter de vous retrouver avec des appels réseau qui survivraient à votre invocation. Utilisez un `CancellationToken` avec un client partagé plutôt que de créer un nouveau client par invocation :

```
using Amazon.S3;

private static readonly IAmazonS3 s3 = new AmazonS3Client();

public async Task<string> FunctionHandler(APIGatewayProxyRequest request,
 ILambdaContext context)
{
    var timeout = context.RemainingTime - TimeSpan.FromMilliseconds(500);
    if (timeout < TimeSpan.FromSeconds(1)) timeout = TimeSpan.FromSeconds(1);

    using var cts = new CancellationTokenSource(timeout);
    await s3.GetObjectAsync("my-bucket", "my-key", cts.Token);
    return "Done";
}
```

Initialisation et arrêt

L'initialisation de la fonction a lieu une fois par environnement d'exécution. Les objets créés lors de l'initialisation sont partagés entre les demandes.

Pour les fonctions Lambda avec extensions, l'environnement d'exécution émet un signal SIGTERM lors de l'arrêt. Ce signal est utilisé par les extensions pour déclencher des tâches de nettoyage, telles que le rinçage des tampons. Vous pouvez vous abonner aux événements SIGTERM pour déclencher des tâches de nettoyage des fonctions, telles que la fermeture des connexions aux bases de données. Pour en savoir plus sur le cycle de vie de l'environnement d'exécution, veuillez consulter the section called “Environnement d’exécution”.

Versions de dépendance

Les instances gérées Lambda nécessitent les versions de package minimales suivantes :

- Amazon.Lambda.Core: version 2.7.1 ou ultérieure
- Amazon.Lambda.RuntimeSupport: version 1.14.1 ou ultérieure
- OpenTelemetry.Instrumentation.AWSLambda: version 1.14.0 ou ultérieure
- AWSXRayRecorder.Core: version 2.16.0 ou ultérieure
- AWSSDK.Core: version 4.0.0.32 ou ultérieure

Outils électriques pour AWS Lambda (.NET)

Powertools for AWS Lambda (.NET) AWS et Distro OpenTelemetry for - Instrumentation DotNet for ne prennent actuellement pas en charge les instances gérées par Lambda.

Étapes suivantes

- Passez en revue l'environnement d'exécution Java pour les instances gérées Lambda
- Vérifier le Node.js temps d'exécution des instances gérées Lambda
- Passez en revue le runtime Python pour les instances gérées Lambda
- En savoir plus sur le dimensionnement des instances gérées Lambda

Support Rust pour les instances gérées Lambda

Configuration de la simultanéité

Le nombre maximum de requêtes simultanées que Lambda envoie à chaque environnement d'exécution est contrôlé par le `PerExecutionEnvironmentMaxConcurrency` paramètre de la configuration de la fonction. Il s'agit d'un paramètre facultatif, et la valeur par défaut pour Rust est de 8 requêtes simultanées par processeur virtuel, ou vous pouvez configurer votre propre valeur.

Cette valeur détermine le nombre de tâches Tokio générées par le runtime et est statique pendant toute la durée de vie de l'environnement d'exécution. Chaque travailleur gère exactement une demande en vol à la fois, sans multiplexage par travailleur. Lambda ajuste automatiquement le nombre de demandes simultanées jusqu'au maximum configuré en fonction de la capacité de chaque environnement d'exécution à absorber ces demandes.

Création de fonctions pour la multisimultanéité

Vous devez appliquer les mêmes pratiques de sécurité des threads lorsque vous utilisez des instances gérées Lambda que dans tout autre environnement multithread. Étant donné que l'objet du gestionnaire est partagé entre tous les threads de travail, tout état mutable doit être sûr pour les threads. Cela inclut les collections, les connexions à la base de données et tous les objets statiques modifiés lors du traitement des demandes.

Pour activer la gestion des demandes simultanées, ajoutez l'indicateur de `concurrency-tokio` fonctionnalité à votre `Cargo.toml` fichier.

```
[dependencies]
lambda_runtime = { version = "1", features = ["concurrency-tokio"] }
```

Le point `lambda_runtime::run_concurrent(…)` d'entrée doit être appelé depuis un environnement d'exécution Tokio, généralement fourni par l'`#[tokio::main]`attribut de votre fonction principale. La fermeture de votre gestionnaire doit implémenter Clone + Send. Cela permet au framework de partager votre gestionnaire entre plusieurs tâches asynchrones en toute sécurité. Si ces limites ne sont pas respectées, votre code ne sera pas compilé.

Lorsque vous avez besoin d'un état partagé entre plusieurs invocations (un pool de base de données, une structure de configuration), enveloppez-le dans Arc et clonez-le `Arc` dans chaque invocation.

Tous les AWS SDK pour les clients Rust sont sécurisés en matière de concurrence et ne nécessitent aucune manipulation particulière.

Exemple : AWS Client du SDK

L'exemple suivant utilise un client S3 pour charger un objet à chaque appel. Le client est cloné directement dans la fermeture sans `Arc` :

```
let config = aws_config::load_defaults(BehaviorVersion::latest()).await;
let s3_client = aws_sdk_s3::Client::new(&config);
```

```
run_concurrent(service_fn(move |event: LambdaEvent<Request>| {
    let s3_client = s3_client.clone(); // cheap clone, no Arc needed
    async move {
        s3_client.put_object()
            .bucket(&event.payload.bucket)
            .key(&event.payload.key)
            .body(event.payload.body.into_bytes().into())
            .send()
            .await?;
        Ok(Response { message: "uploaded".into() })
    }
}))
.await
```

Exemple : pools de connexions à la base de données

Lorsque votre gestionnaire a besoin d'accéder à un état partagé, tel qu'un client et une configuration, enveloppez-le dans Arc et clonez-le `Arc` dans chaque invocation :

```
#[derive(Debug)]
struct AppState {
    dynamodb_client: DynamoDbClient,
    table_name: String,
    cache_ttl: Duration,
}

let config = aws_config::load_defaults(BehaviorVersion::latest()).await;
let state = Arc::new(AppState {
    dynamodb_client: DynamoDbClient::new(&config),
    table_name: std::env::var("TABLE_NAME").expect("TABLE_NAME must be set"),
    cache_ttl: Duration::from_secs(300),
});

run_concurrent(service_fn(move |event: LambdaEvent<Request>| {
    let state = state.clone();
    async move { handle(event, state).await }
}))
.await
```

Répertoire /tmp partagé

Le `/tmp` répertoire est partagé entre toutes les invocations simultanées dans le même environnement d'exécution. Utilisez des noms de fichiers uniques par appel (par exemple, incluez l'ID

de demande) ou implémentez un verrouillage explicite des fichiers pour éviter toute corruption des données.

Logging

L'entrelacement des journaux (les entrées de journal provenant de différentes demandes sont entrelacées dans les journaux) est normal dans les systèmes multisimultanés. Les fonctions utilisant les instances gérées Lambda prennent en charge le format de journal JSON structuré via les contrôles de journalisation avancés de Lambda. Ce format inclut le`requestId`, permettant de corréler les entrées du journal à une seule demande. Pour plus d'informations, voirthe section called “Implémentation de la journalisation avancée avec la caisse Tracing”.

Contexte de la demande

L'`Context`objet est transmis directement à chaque appel de gestionnaire. Permet `event.context.request_id` d'accéder à l'ID de demande pour la demande en cours.

Utilisez-le `event.context.xray_trace_id` pour accéder à l'ID de X-Ray trace. Lambda ne prend pas en charge la variable d'`_X_AMZN_TRACE_ID`environnement avec les instances gérées Lambda. L'ID de X-Ray trace est propagé automatiquement lors de l'utilisation du AWS SDK pour Rust.

Utilisée `event.context.deadline` pour détecter les délais d'invocation : elle contient la date limite d'invocation en millisecondes.

Initialisation et arrêt

L'initialisation des fonctions se produit une fois par environnement d'exécution. Les objets créés lors de l'initialisation sont partagés entre les requêtes.

Pour les fonctions Lambda dotées d'extensions, l'environnement d'exécution émet un signal SIGTERM lors de l'arrêt. Ce signal est utilisé par les extensions pour déclencher des tâches de nettoyage, telles que le vidage des buffers. `lambda_runtime`propose une aide pour simplifier la configuration de la gestion gracieuse des signaux d'arrêt, spawn_graceful_shutdown_handler (). Pour en savoir plus sur le cycle de vie de l'environnement d'exécution, veuillez consulter the section called “Environnement d’exécution”.

Versions de dépendance

Les instances gérées Lambda nécessitent la version minimale du package suivante :

- `lambda_runtime`: version 1.1.1 ou ultérieure, avec la `concurrency-tokio` fonctionnalité activée

- La version minimale de Rust (MSRV) prise en charge est 1.84.0.

Mise en réseau pour les instances gérées par Lambda

Lorsque vous exécutez les fonctions d'instances gérées Lambda, vous devez configurer la connectivité réseau pour permettre à vos fonctions d'événement Lambda d'accéder à des ressources en dehors du VPC. Cela inclut des AWS services tels qu'Amazon S3 et DynamoDB. La connectivité est également nécessaire pour transmettre des données de télémétrie à CloudWatch Logs and. X-Ray

Options de connectivité

Il existe trois approches principales pour configurer la connectivité VPC, chacune avec des compromis différents en termes de coût, de sécurité et de complexité.

Sous-réseau public avec passerelle Internet

Cette option utilise un sous-réseau public avec un accès direct à Internet via une passerelle Internet. Vous pouvez choisir entre les configurations IPv4 et IPv6.

IPv4 avec passerelle Internet

Pour configurer la connectivité IPv4 avec une passerelle Internet

1. Créez ou utilisez un sous-réseau public existant avec un bloc d'adresse CIDR IPv4.
2. Attachez une passerelle Internet à votre VPC.
3. Mettez à jour la table de routage pour acheminer le `0.0.0.0/0` trafic vers la passerelle Internet.
4. Assurez-vous que les ressources disposent d'adresses IPv4 publiques ou d'adresses IP élastiques attribuées.
5. Configurez les groupes de sécurité pour autoriser le trafic sortant sur les ports requis.

Cette configuration fournit une connectivité bidirectionnelle, autorisant à la fois les connexions sortantes depuis vos fonctions et les connexions entrantes depuis Internet.

IPv6 avec passerelle Internet

Pour configurer la connectivité IPv6 avec une passerelle Internet

1. Activez IPv6 sur votre VPC.
2. Créez ou utilisez un sous-réseau public existant auquel un bloc d'adresse CIDR IPv6 est attribué.
3. Connectez une passerelle Internet à votre VPC (la même passerelle Internet peut gérer à la fois IPv4 et IPv6).
4. Mettez à jour la table de routage pour acheminer le `::/0` trafic vers la passerelle Internet.
5. Vérifiez que les AWS services auxquels vous devez accéder sont compatibles avec le protocole IPv6 dans votre région.
6. Configurez les groupes de sécurité pour autoriser le trafic sortant sur les ports requis.

Cette configuration fournit une connectivité bidirectionnelle à l'aide de l'adressage IPv6.

IPv6 avec passerelle Internet de sortie uniquement

Pour configurer la connectivité IPv6 avec une passerelle Internet de sortie uniquement

1. Activez IPv6 sur votre VPC.
2. Créez ou utilisez un sous-réseau public existant auquel un bloc d'adresse CIDR IPv6 est attribué.
3. Associez une passerelle Internet de sortie uniquement à votre VPC.
4. Mettez à jour la table de routage pour acheminer le `::/0` trafic vers la passerelle Internet de sortie uniquement.
5. Vérifiez que les AWS services auxquels vous devez accéder sont compatibles avec le protocole IPv6 dans votre région.
6. Configurez les groupes de sécurité pour autoriser le trafic sortant sur les ports requis.

Cette configuration fournit une connectivité sortante uniquement, empêchant les connexions entrantes en provenance d'Internet tout en permettant à vos fonctions d'initier des connexions sortantes.

Points de terminaison d’un VPC

Les points de terminaison VPC vous permettent de connecter en privé votre VPC aux AWS services pris en charge sans avoir besoin d'une passerelle Internet, d'un périphérique NAT, d'une connexion VPN ou d'une connexion Direct Connect. AWS Le trafic entre votre VPC et le AWS service ne quitte pas le réseau Amazon.

Pour configurer les points de terminaison VPC

1. Ouvrez la console Amazon VPC à l'adresse console.aws.amazon. com/vpc/.
2. Dans le panneau de navigation, choisissez Points de terminaison.
3. Choisissez Créer un point de terminaison.
4. Pour Service category (Catégorie de service), choisissez Services AWS .
5. Dans Nom du service, sélectionnez le point de terminaison de service dont vous avez besoin (par exemple, `com.amazonaws.region.s3` pour Amazon S3).
6. Pour VPC, sélectionnez votre VPC.
7. Pour les sous-réseaux, sélectionnez les sous-réseaux dans lesquels vous souhaitez créer des interfaces réseau de point de terminaison. Pour assurer la haute disponibilité, sélectionnez les sous-réseaux dans plusieurs zones de disponibilité.
8. Pour Security groups (Groupes de sécurité), sélectionnez les groupes de sécurité à associer aux interfaces réseau du point de terminaison. Les groupes de sécurité doivent autoriser le trafic entrant en provenance du groupe de sécurité de votre fonction sur les ports requis.
9. Choisissez Créer un point de terminaison.

Répétez ces étapes pour chaque AWS service auquel vos fonctions doivent accéder.

Sous-réseau privé avec passerelle NAT

Cette option utilise une passerelle NAT pour fournir un accès Internet aux ressources des sous-réseaux privés tout en préservant la confidentialité des ressources.

Pour configurer un sous-réseau privé avec une passerelle NAT

1. Créez un sous-réseau public (s'il n'en existe pas déjà un) avec un bloc CIDR.
2. Attachez une passerelle Internet à votre VPC.
3. Créez une passerelle NAT dans le sous-réseau public et attribuez une adresse IP élastique.
4. Mettez à jour la table de routage du sous-réseau public pour ajouter une route : `0.0.0.0/0` → passerelle Internet.
5. Créez ou utilisez un sous-réseau privé existant avec un bloc CIDR.
6. Mettez à jour la table de routage du sous-réseau privé pour ajouter une route : `0.0.0.0/0` → passerelle NAT.
7. Configurez les groupes de sécurité pour autoriser le trafic sortant sur les ports requis.

Pour une haute disponibilité, déployez une passerelle NAT dans chaque zone de disponibilité et configurez des tables de routage par zone de disponibilité pour utiliser la passerelle NAT locale. Cela permet d'éviter les frais de transfert de données entre AZ et d'améliorer la résilience.

Choix d'une option de connectivité

Tenez compte des facteurs suivants lorsque vous choisissez une option de connectivité :

Sous-réseau public avec passerelle Internet

- Configuration la plus simple au moindre coût
- Adapté aux environnements de développement et de test
- Les ressources peuvent recevoir des connexions entrantes depuis Internet (considérations de sécurité)
- Supporte à la fois IPv4 et IPv6

Points de terminaison d'un VPC

- Sécurité maximale, le trafic reste sur le AWS réseau
- Latence plus faible par rapport au routage Internet
- Recommandé pour les environnements de production soumis à des exigences de sécurité strictes
- Coût plus élevé par point de terminaison, par zone de disponibilité et par Go traité
- Nécessite un point de terminaison dans chaque zone de disponibilité pour une haute disponibilité

Sous-réseau privé avec passerelle NAT

- Les ressources restent privées sans accès Internet entrant
- Modèle d'architecture d'entreprise standard
- Supporte tout le trafic Internet IPv4
- Coût modéré avec frais horaires de passerelle NAT et frais de traitement des données
- Supporte uniquement IPv4

Étapes suivantes

- En savoir plus sur les fournisseurs de capacité pour les instances gérées Lambda

- Comprendre le dimensionnement pour les instances gérées Lambda
- Consultez les guides spécifiques à l'exécution pour Java et Node.jsPython
- Comprendre la sécurité et les autorisations pour les instances gérées Lambda

Surveillance des instances gérées Lambda

Lambda fournit deux types de données de surveillance à vos fournisseurs de capacité : les métriques et les journaux système. Ensemble, ils vous offrent une visibilité sur l'utilisation des ressources, les événements liés au cycle de vie des instances et les problèmes opérationnels.

- Métriques : Lambda publie automatiquement CloudWatch des mesures pour vos fournisseurs de capacité afin de vous aider à surveiller l'utilisation des ressources, à suivre les coûts et à optimiser les performances. Pour de plus amples informations, veuillez consulter CloudWatch métriques pour les instances gérées Lambda.
- Journaux système : Lambda envoie automatiquement des journaux système à des CloudWatch journaux qui enregistrent les événements et les erreurs liés au cycle de vie des instances pour votre fournisseur de capacité. Pour de plus amples informations, veuillez consulter Journaux système du fournisseur de capacité pour les instances gérées Lambda.

CloudWatch métriques pour les instances gérées Lambda

Vous pouvez surveiller les instances gérées Lambda à l'aide de CloudWatch métriques. Lambda publie automatiquement des mesures pour vous aider CloudWatch à surveiller l'utilisation des ressources, à suivre les coûts et à optimiser les performances.

Métriques disponibles

Les instances gérées Lambda fournissent des mesures à deux niveaux : au niveau du fournisseur de capacité et au niveau de l'environnement d'exécution.

Indicateurs au niveau du fournisseur de capacité

Les indicateurs au niveau du fournisseur de capacité fournissent une visibilité sur l'utilisation globale des ressources sur l'ensemble de vos instances. Ces mesures utilisent les dimensions suivantes :

- CapacityProviderName- Le nom de votre fournisseur de capacité
- InstanceType- Le type d'instance EC2

Les mesures d'utilisation des ressources suivantes sont disponibles :

- CPUUtilization : pourcentage d'utilisation du processeur entre les instances du fournisseur de capacité
- MemoryUtilization- Le pourcentage d'utilisation de la mémoire entre les instances du fournisseur de capacité

Les indicateurs de capacité suivants sont disponibles :

- vCPUAvailable - La quantité de vCPU disponible sur les instances à allouer (en nombre)
- MemoryAvailable- La quantité de mémoire disponible sur les instances pour l'allocation (en octets)
- vCPUAllocated - La quantité de vCPU allouée aux instances pour les environnements d'exécution (en nombre)
- MemoryAllocated- La quantité de mémoire allouée aux instances pour les environnements d'exécution (en octets)

Mesures au niveau de l'environnement d'exécution

Les métriques au niveau de l'environnement d'exécution fournissent une visibilité sur l'utilisation des ressources et la simultanéité pour les différentes fonctions. Ces mesures utilisent les dimensions suivantes :

- CapacityProviderName- Le nom de votre fournisseur de capacité
- FunctionName- Le nom de votre fonction Lambda
- Ressource : par ressource, affichez les métriques d'une version spécifique d'une fonction.

> **Note**
>
> Pour les instances gérées Lambda (LMI), la `Resource` dimension ne prend en charge que les versions de fonctions. Le format est `<FunctionName>:<FunctionVersion>`.

Métriques de l'environnement d'exécution disponibles :

- ExecutionEnvironmentConcurrency- La simultanéité maximale sur une période d'échantillonnage d'une minute

- ExecutionEnvironmentConcurrencyLimit- La limite maximale de simultanéité par environnement d'exécution
- ExecutionEnvironmentCPUUtilization- Le pourcentage d'utilisation du processeur pour les environnements d'exécution de la fonction
- ExecutionEnvironmentMemoryUtilization- Le pourcentage d'utilisation de la mémoire pour les environnements d'exécution de la fonction

Indicateurs des raisons de l'étranglement

Les instances gérées Lambda émettent des mesures granulaires relatives à la raison de l'étranglement qui identifient la contrainte de ressources à l'origine de l'étranglement. Pour chaque accélérateur, Lambda émet exactement l'une des sous-métriques suivantes avec une valeur de 1, tandis que les trois autres sont émises avec une valeur de 0 :

- ConcurrencyThrottles— L'environnement d'exécution a atteint sa limite maximale de simultanéité. Cela peut être résolu en augmentant ExecutionEnvironmentMaxConcurrency ou en dimensionnant les environnements d'exécution de manière plus agressive.
- CPUThrottles — L'environnement d'exécution a épuisé les ressources CPU qui lui étaient allouées. Vous pouvez y remédier en augmentant l'allocation de processeurs virtuels de votre fonction ou en réduisant la charge par environnement ExecutionEnvironmentMaxConcurrency pour la réduire.
- MemoryThrottles— L'environnement d'exécution a épuisé la mémoire allouée. Vous pouvez y remédier en augmentant l'allocation mémoire de votre fonction ou en réduisant la charge par environnement ExecutionEnvironmentMaxConcurrency pour la réduire.
- DiskThrottles— L'environnement d'exécution a épuisé l'espace disque qui lui était alloué. Vous pouvez y remédier en augmentant le stockage éphémère de votre fonction ou en réduisant la charge par environnement ExecutionEnvironmentMaxConcurrency pour la réduire.

Lambda émet toujours la `Throttles` métrique standard à côté de ces sous-métriques. Utilisez ces indicateurs pour comprendre pourquoi votre fonction évolue et s'il convient d'ajuster votre simultanéité maximale, la mémoire de fonction, l'allocation de processeurs virtuels ou la configuration des disques. Pour obtenir la liste complète des métriques Lambda, consultezTypes de métriques pour les fonctions d'événement Lambda.

Fréquence et rétention métriques

Les métriques Lambda Managed Instances sont publiées à intervalles d'une minute et conservées pendant 15 mois.

Affichage des statistiques dans CloudWatch

Pour afficher les métriques des instances gérées Lambda dans la console CloudWatch

1. Ouvrez la CloudWatch console à l'adresse console.aws.amazon. com/cloudwatch/.
2. Dans le panneau de navigation, sélectionnez Métriques.
3. Dans l'onglet Toutes les mesures, choisissez AWS/Lambda.
4. Choisissez la dimension métrique que vous souhaitez afficher :
   - Pour les mesures au niveau du fournisseur de capacité, filtrez par CapacityProviderName et InstanceType
   - Pour les mesures au niveau de l'environnement d'exécution, filtrez par CapacityProviderName FunctionName, et par ressource
5. Sélectionnez les indicateurs que vous souhaitez surveiller.

Utilisation de métriques pour optimiser les performances

Surveillez l'utilisation du processeur et de la mémoire pour déterminer si vos fonctions sont correctement dimensionnées. Un taux d'utilisation élevé peut indiquer le besoin de types d'instances plus volumineux ou d'une allocation de mémoire de fonction accrue. Suivez les indicateurs de simultanéité pour comprendre le comportement de mise à l'échelle et identifier les éventuelles limitations.

Surveillez les indicateurs de capacité pour vérifier que des ressources suffisantes sont disponibles pour vos charges de travail. Le vCPU disponible et MemoryAvailable les métriques vous aident à comprendre la capacité restante de vos instances.

Étapes suivantes

- En savoir plus sur la mise à l'échelle des instances gérées Lambda
- Consultez les guides spécifiques à l'exécution pour Java et Node.js Python ???
- Configurez la connectivité VPC pour vos fournisseurs de capacité
- Comprendre la sécurité et les autorisations pour les instances gérées Lambda

Journaux système du fournisseur de capacité pour les instances gérées Lambda

Pour vous aider à surveiller et à dépanner votre environnement Lambda Managed Instances, Lambda génère automatiquement des journaux système pour vos fournisseurs de capacité. Vous pouvez consulter les journaux des fournisseurs de capacité à l'aide de la console Lambda, de la CloudWatch console, du AWS Command Line Interface (AWS CLI) ou de l' CloudWatch API. Vous pouvez également acheminer les journaux vers Amazon S3 et Firehose à l'aide CloudWatch des filtres d'abonnement aux journaux.

Tant que le rôle d'opérateur de votre fournisseur de capacité dispose des autorisations nécessaires, Lambda capture les journaux système et les envoie à Amazon CloudWatch Logs, qui est la destination par défaut.

> **Note**
>
> Les journaux système du fournisseur de capacité sont activés par défaut. Lambda envoie automatiquement les journaux système à CloudWatch Logs lorsque vous créez un fournisseur de capacité.

- CloudWatch Logs est la destination de journalisation par défaut pour les journaux système du fournisseur de capacité. CloudWatch Logs fournit des fonctionnalités de visualisation et d'analyse des journaux en temps réel, ainsi que la prise en charge de la création de mesures et d'alarmes en fonction des données de vos journaux.
- Amazon S3 est économique pour le stockage à long terme, et des services comme Athena peuvent être utilisés pour analyser les journaux. La latence est généralement plus élevée.
- Firehose propose une diffusion en continu gérée des journaux vers différentes destinations. Si vous devez envoyer des journaux à d'autres AWS services (par exemple, OpenSearch Service ou API Redshift Data) ou à des plateformes tierces (telles que Datadog, New Relic ou Splunk), Firehose simplifie ce processus en proposant des intégrations prédéfinies.

Configuration des destinations de journal

Lambda prend en charge plusieurs destinations pour les journaux système de votre fournisseur de capacité. Quelle que soit la destination que vous avez choisie, Lambda propose des options pour contrôler le filtrage et la diffusion des journaux.

Les journaux système des fournisseurs de capacité utilisent exclusivement le format structuré JSON. Les journaux structurés JSON offrent une meilleure capacité de recherche et permettent une analyse automatique. Vous pouvez contrôler les journaux que Lambda envoie à la destination de votre choix en configurant le niveau de journalisation du système. Le filtrage vous aide à gérer les coûts de stockage et trouver plus facilement les entrées de journal pertinentes lors du débogage.

Pour plus d'informations sur la configuration de chaque destination, consultez les rubriques suivantes :

- Envoi des journaux du système du fournisseur de capacité à CloudWatch Logs
- Envoi des journaux système du fournisseur de capacité à Firehose
- Envoi des journaux système du fournisseur de capacité à Amazon S3

Configuration des contrôles de journalisation pour les fournisseurs de capacité

Pour vous permettre de mieux contrôler la façon dont les journaux système de votre fournisseur de capacité sont capturés, traités et consommés, Lambda propose les options de configuration de journalisation suivantes :

- Niveau de journalisation : choisissez le niveau de détail des journaux système que Lambda envoie à CloudWatch Logs : `DEBUG`, `INFO`, ou `WARN`.
- Groupe de journaux : choisissez le groupe de CloudWatch journaux auquel votre fournisseur de capacité envoie les journaux.

Pour plus d'informations sur la configuration des contrôles de journalisation, consultez les rubriques suivantes :

- Log-level filtrage des journaux système du fournisseur de capacité
- Format de journal système du fournisseur de capacité
- Référence des événements du journal système du fournisseur de capacité

Format de journal système du fournisseur de capacité

Les journaux système du fournisseur de capacité utilisent le format JSON structuré. Les journaux structurés JSON offrent une meilleure facilité de recherche et permettent une analyse automatique des événements opérationnels de votre fournisseur de capacité.

Format JSON pour les journaux du système

Chaque entrée du journal système est capturée sous la forme d'un objet JSON contenant des paires clé-valeur avec les champs de niveau supérieur suivants :

Champ	Type	Description
`timestamp`	String	Heure à laquelle l'événement du journal a été généré, au format ISO 8601.
`level`	String	Le niveau de journalisation de l'événement.
`message`	String	Une description lisible par l'homme de l'événement.
`metadata`	Objet	Des métadonnées structurées relatives à l'événement. Contient des champs qui varient selon le type d'événement.

Champs de métadonnées

L'`metadata`objet contient les champs suivants. Tous les champs ne sont pas présents dans tous les événements.

Champ	Type	Description
`instanceId`	String	L'ID d'instance Amazon EC2 associé à l'événement.
`availabilityZones`	Tableau de chaînes	La ou les zones de disponibilité associées à l'événement.
`instanceTypes`	Tableau de chaînes	Le ou les types d'instance Amazon EC2 associés à l'événement.
`capacityProviderArn`	String	L'ARN du fournisseur de capacité.

Exemple d'entrée de journal

L'exemple suivant montre une entrée de journal système pour un lancement d'instance réussi :

```
{
  "timestamp": "2025-07-01T14:31:15.456Z",
  "level": "INFO",
  "message": "Successfully launched c7g.xlarge instance i-0abc123def456789 in us-
east-1a",
  "metadata": {
    "instanceId": "i-0abc123def456789",
    "availabilityZones": ["us-east-1a"],
    "instanceTypes": ["c7g.xlarge"],
    "capacityProviderArn": "arn:aws:lambda:us-east-1:123456789012:capacity-provider:my-
capacity-provider"
  }
}
```

Log-level filtrage des journaux système du fournisseur de capacité

Lambda peut filtrer les journaux système de votre fournisseur de capacité afin que seuls les journaux d'un certain niveau de détail ou inférieur soient envoyés à CloudWatch Logs. Vous pouvez choisir entre les niveaux de journalisation suivants.

Niveau de journalisation	Usage
DEBUG (le plus détaillé)	Informations détaillées pour le débogage du système
INFO	Messages qui enregistrent le fonctionnement normal du fournisseur de capacité
WARN (moindre détail)	Messages concernant des erreurs potentielles susceptibles d'entraîner un comportement inattendu si elles ne sont pas corrigées

Lorsque vous sélectionnez un niveau de journal, Lambda envoie des journaux à ce niveau ou à un niveau inférieur. Par exemple, si vous définissez le niveau de journalisation système d'un fournisseur de capacité sur INFO, Lambda n'envoie pas de sorties de journal au niveau DEBUG.

Par défaut, Lambda définit le niveau de journalisation du système sur INFO. Pour recevoir des journaux plus détaillés, réglez le niveau sur DEBUG. Pour recevoir moins de journaux, réglez le niveau sur WARN. Pour consulter la liste des niveaux de journalisation auxquels Lambda mappe les différents événements du journal système, consultez. Référence des événements du journal système du fournisseur de capacité

Configuration du niveau de journalisation du système

Pour configurer le niveau de journalisation du système pour votre fournisseur de capacité, vous pouvez utiliser la console Lambda ou le AWS Command Line Interface (AWS CLI). Vous pouvez également configurer le niveau de journalisation du système à l'aide des commandes de l'API `CreateCapacityProvider` et `UpdateCapacityProvider` Lambda.

Pour configurer le niveau de journalisation du système (console)

1. Ouvrez la page des fournisseurs de capacité de la console Lambda.
2. Choisissez un fournisseur de capacité.
3. Sélectionnez Additional configuration (Configuration supplémentaire).
4. Dans la section Configuration de la journalisation, choisissez Modifier.
5. Sélectionnez le niveau de journalisation système souhaité pour votre fournisseur de capacité.
6. Choisissez Enregistrer.

Pour définir le niveau de journalisation du système lors de la création d'un fournisseur de capacité (AWS CLI)

- Pour configurer le niveau de journalisation du système lorsque vous créez un nouveau fournisseur de capacité, utilisez l'`--telemetry-config`option de la commande create-capacity provider. A défini `SystemLogLevel` sur l'une des valeurs `DEBUG`, `INFO` ou `WARN`.

```
aws lambda create-capacity-provider \
  --capacity-provider-name my-capacity-provider \
  --vpc-config SubnetIds=subnet-12345,subnet-67890,SecurityGroupIds=sg-12345 \
  --permissions-config
 CapacityProviderOperatorRoleArn=arn:aws:iam::123456789012:role/MyOperatorRole \
  --telemetry-config LoggingConfig={SystemLogLevel=DEBUG}
```

Pour mettre à jour le niveau de journalisation système d'un fournisseur de capacité existant (AWS CLI)

- Pour modifier le niveau de journalisation système d'un fournisseur de capacité existant, utilisez la commande update-capacity provider.

```
aws lambda update-capacity-provider \
  --capacity-provider-name my-capacity-provider \
  --telemetry-config LoggingConfig={SystemLogLevel=WARN}
```

Référence des événements du journal système du fournisseur de capacité

Lambda publie les événements du journal système pour les opérations liées au cycle de vie des instances du fournisseur de capacité. Le tableau suivant indique les événements publiés par Lambda et indique si chaque événement est enregistré en fonction du niveau de journalisation du système que vous avez configuré.

Pour plus d'informations sur la configuration du niveau de journalisation du système, consultezLog-level filtrage des journaux système du fournisseur de capacité. Pour plus de détails sur le format des entrées de journal, consultezFormat de journal système du fournisseur de capacité.

Cartographie du niveau des événements du journal système

Événement	Description	**DEBUG**	**INFO**	**WARN**
Lancement	Émis lorsque Lambda lance un lancement d'instance pour le fournisseur de capacité.	Connecté	Connecté	Non connecté
Lancé	Émis lorsqu'une instance passe avec succès à un état actif et est prête à servir des invocations.	Connecté	Connecté	Non connecté
LaunchFailed	Émis lorsqu'une tentative de lancement d'instance échoue.	Connecté	Connecté	Connecté
Résiliation	Émis lorsque Lambda marque une instance à terminer.	Connecté	Connecté	Non connecté

Événement	Description	DEBUG	INFO	WARN
Terminated (Résilié)	Émis lorsqu'une instance est terminée avec succès.	Connecté	Connecté	Non connecté
TerminateFailed	Émis lorsque Lambda ne parvient pas à terminer une instance.	Connecté	Connecté	Connecté
HealthCheckFailed	Émis lorsqu'une instance échoue à son contrôle de santé et est marquée comme étant défectueu se.	Connecté	Connecté	Connecté

> **Note**
>
> Cette liste s'allonge au fur et à mesure que Lambda ajoute de nouvelles fonctionnalités de fournisseur de capacité.

Envoi des journaux du système du fournisseur de capacité à CloudWatch Logs

Par défaut, Lambda capture automatiquement les journaux système de votre fournisseur de capacité et les envoie à CloudWatch Logs, à condition que le rôle d'opérateur de votre fournisseur de capacité dispose des autorisations nécessaires. Ces journaux sont stockés dans un groupe de journaux nommé`/aws/lambda/capacity-provider/<capacity-provider-name>`. Si nécessaire, vous pouvez configurer votre fournisseur de capacité pour envoyer des journaux à un autre groupe de journaux à l'aide de la console Lambda ou de l' AWS CLI API Lambda. Pour de plus amples informations, veuillez consulter Configuration des groupes de CloudWatch journaux.

Vous pouvez consulter les journaux de votre fournisseur de capacité à l'aide de la console Lambda, de la CloudWatch console, du AWS Command Line Interface (AWS CLI) ou de l' CloudWatch API. Pour de plus amples informations, veuillez consulter Affichage CloudWatch des journaux pour les fournisseurs de capacité.

Autorisations IAM requises

Le rôle d'opérateur de votre fournisseur de capacité nécessite les autorisations suivantes pour télécharger des CloudWatch journaux dans Logs :

- `logs:CreateLogGroup`
- `logs:CreateLogStream`
- `logs:PutLogEvents`

Pour en savoir plus, consultez la section Utilisation de politiques basées sur l'identité (politiques IAM) pour les CloudWatch journaux dans le guide de l'utilisateur Amazon CloudWatch .

Vous pouvez ajouter ces autorisations de CloudWatch journalisation à l'aide de la politique `AWSLambdaManagedEC2ResourceOperator` AWS gérée fournie par Lambda. Exécutez la commande suivante pour ajouter cette politique à votre rôle :

```
aws iam attach-role-policy --role-name your-role --policy-arn arn:aws:iam::aws:policy/
AWSLambdaManagedEC2ResourceOperator
```

Pour de plus amples informations, veuillez consulter the section called “Rôle d'opérateur”.

> **Important**
>
> Si le rôle d'opérateur ne dispose pas des autorisations requises, Lambda ne fournit pas de journaux système et ne renvoie pas d'erreur. Assurez-vous que votre rôle d'opérateur dispose des autorisations appropriées pour éviter les échecs de livraison silencieuse des journaux.

Tarification

L'utilisation des journaux système du fournisseur de capacité est gratuite ; toutefois, des frais de CloudWatch journalisation standard s'appliquent. Pour en savoir plus, consultez PricingCloudWatch (Tarification).

Configuration des groupes de CloudWatch journaux

Par défaut, Lambda crée un groupe de journaux portant le nom `/aws/lambda/capacity-provider/<capacity-provider-name>` de votre fournisseur de capacité. Pour envoyer des journaux à un autre groupe de journaux, utilisez la console Lambda ou AWS CLI les commandes de l'`UpdateCapacityProvider`API `CreateCapacityProvider` and.

Lorsque vous configurez un groupe de journaux personnalisé, son nom doit respecter les règles de dénomination CloudWatch des journaux. De plus, les noms de groupes de journaux personnalisés ne doivent pas commencer par cette chaîne`aws/`. Si vous créez un groupe de journaux personnalisé

commençant paraws/, Lambda ne peut pas créer le groupe de journaux et votre fournisseur de capacité n'envoie pas de journaux à CloudWatch.

Flux de journaux

Au sein du groupe de journaux, Lambda crée des flux de journaux en utilisant le format de dénomination suivant :

```
<capacity-provider-name>/managed-instances
```

Par exemple, pour un fournisseur de capacité nommémy-capacity-provider, le flux de log est le suivant :

```
my-capacity-provider/managed-instances
```

Configuration d'un groupe de journaux personnalisé

Pour modifier le groupe de journaux d'un fournisseur de capacité (console)

1. Ouvrez la page des fournisseurs de capacité de la console Lambda.
2. Choisissez un fournisseur de capacité.
3. Sélectionnez Additional configuration (Configuration supplémentaire).
4. Dans la section Configuration de la journalisation, choisissez Modifier.
5. Entrez le nom du groupe de CloudWatch journaux auquel vous souhaitez que votre fournisseur de capacité envoie des journaux. Si vous entrez le nom d'un groupe de journaux existant, votre fournisseur de capacité utilise ce groupe. S'il n'existe aucun groupe de journaux portant le nom que vous avez saisi, Lambda crée un nouveau groupe de journaux portant ce nom.
6. Choisissez Enregistrer.

Pour modifier le groupe de journaux d'un fournisseur de capacité (AWS CLI)

- Pour modifier le groupe de journaux d'un fournisseur de capacité existant, utilisez la commande update-capacity provider.

```
aws lambda update-capacity-provider \
  --capacity-provider-name my-capacity-provider \
  --telemetry-config LoggingConfig={LogGroup=myLogGroup}
```

Pour spécifier un groupe de journaux personnalisé lorsque vous créez un fournisseur de capacité (AWS CLI)

- Pour spécifier un groupe de journaux personnalisé lorsque vous créez un nouveau fournisseur de capacité, utilisez l'`--telemetry-config`option de la commande create-capacity provider.

```
aws lambda create-capacity-provider \
  --capacity-provider-name my-capacity-provider \
  --vpc-config SubnetIds=subnet-12345,subnet-67890,SecurityGroupIds=sg-12345 \
  --permissions-config
 CapacityProviderOperatorRoleArn=arn:aws:iam::123456789012:role/MyOperatorRole \
  --telemetry-config LoggingConfig={LogGroup=myLogGroup}
```

Autorisations relatives au rôle d'opérateur

Pour que votre fournisseur de capacité puisse envoyer des CloudWatch journaux à Logs, le rôle d'opérateur doit disposer de l'PutLogEventsautorisation logs :. Lambda n'ajoute pas cette autorisation automatiquement. Si ce n'est pas déjà fait pour le rôle d'opérateur, ajoutez-le avant de créer le fournisseur de capacité. Cette autorisation est incluse dans la politique `AWSLambdaManagedEC2ResourceOperator` gérée.

Pour plus d'informations sur le rôle de l'opérateur, consultezthe section called “Rôle d'opérateur”.

Affichage CloudWatch des journaux pour les fournisseurs de capacité

Vous pouvez consulter les CloudWatch journaux Amazon Logs de votre fournisseur de capacité à l'aide de la console Lambda, de la CloudWatch console ou du AWS Command Line Interface (AWS CLI). Suivez les instructions des sections suivantes pour accéder aux journaux de votre fournisseur de capacité.

Streamez des CloudWatch journaux avec Logs Live Tail

Amazon CloudWatch Logs Live Tail vous aide à dépanner rapidement vos fournisseurs de capacité en affichant une liste en streaming des nouveaux événements de journalisation en temps réel. Vous pouvez consulter et filtrer les journaux ingérés depuis votre fournisseur de capacité, ce qui vous permet de détecter et de résoudre rapidement les problèmes.

> **Note**
>
> Le coût des sessions Live Tail est calculé en fonction du temps d'utilisation de la session, par minute. Pour plus d'informations sur la tarification, consultez la page CloudWatch Tarification Amazon.

Pour démarrer une session Live Tail, ouvrez le groupe de journaux de votre fournisseur de capacité dans la CloudWatch console et choisissez Live Tail. Pour plus d'informations, consultez la section Utiliser Live Tail pour consulter les journaux en temps quasi réel dans le Guide de CloudWatch l'utilisateur Amazon.

Afficher les journaux dans la console Lambda

Pour afficher les journaux dans la console Lambda

1. Ouvrez la page des fournisseurs de capacité de la console Lambda.
2. Choisissez un fournisseur de capacité.
3. Choisissez l'onglet Surveiller.
4. Choisissez Afficher les connexions CloudWatch pour ouvrir le groupe de journaux dans la CloudWatch console.

Afficher les journaux dans la CloudWatch console

Pour afficher les journaux dans la CloudWatch console

1. Ouvrez la CloudWatch console à l'adresse console.aws.amazon. com/cloudwatch/.
2. Dans le volet de navigation, choisissez Journaux, puis Groupes de journaux.
3. Choisissez le groupe de journaux pour votre fournisseur de capacité. Par défaut, le groupe de journaux est nommé`/aws/lambda/capacity-provider/`*`<capacity-provider-name>`*.
4. Choisissez un flux de journal pour afficher les événements du journal.

Afficher les journaux à l'aide du AWS CLI

Pour afficher les journaux à l'aide de AWS CLI, utilisez les `aws logs` commandes. L'exemple suivant extrait les événements de journal les plus récents pour un fournisseur de capacité :

```
aws logs get-log-events \
  --log-group-name /aws/lambda/capacity-provider/my-capacity-provider \
  --log-stream-name my-capacity-provider/managed-instances
```

Vous pouvez également utiliser CloudWatch Logs Insights pour interroger et analyser les journaux système de votre fournisseur de capacité. Les exemples de requêtes suivants concernent tous les événements de niveau ERROR :

```
aws logs start-query \
  --log-group-name /aws/lambda/capacity-provider/my-capacity-provider \
  --start-time $(date -d '1 hour ago' +%s) \
  --end-time $(date +%s) \
  --query-string 'fields @timestamp, @message | filter level = "ERROR" | sort
 @timestamp desc'
```

Envoi des journaux système du fournisseur de capacité à Firehose

Vous pouvez envoyer les journaux système du fournisseur de capacité à Amazon Data Firehose. Avec Firehose, vous pouvez diffuser des journaux en temps réel vers différentes destinations, y compris des outils d'analyse tiers et des points de terminaison personnalisés.

> **Note**
>
> Vous pouvez configurer les journaux système du fournisseur de capacité à envoyer à Firehose à l'aide des AWS kits SDK et de AWS CLI tous les kits de développement logiciel. AWS CloudFormation

Tarification

Pour plus d'informations sur la tarification, consultez la page CloudWatch Tarification Amazon.

Configuration de la livraison des journaux Firehose

Pour envoyer les journaux système du fournisseur de capacité à Firehose, créez un filtre d'abonnement CloudWatch aux journaux dans le groupe de journaux de votre fournisseur de capacité. Le filtre d'abonnement achemine les événements du journal vers votre flux de diffusion Firehose.

Par défaut, le groupe de journaux de votre fournisseur de capacité est nommé`/aws/lambda/capacity-provider/<capacity-provider-name>`. Utilisez ce groupe de journaux lors de la création du filtre d'abonnement.

Pour obtenir des instructions sur la configuration d'un filtre d'abonnement pour Firehose, y compris la création de rôles et les autorisations IAM, consultez la section Filtres d'abonnement avec Firehose dans le guide de l'utilisateur Amazon CloudWatch .

Cross-account journalisation

Vous pouvez configurer votre fournisseur de capacité pour envoyer des journaux à un flux de diffusion Firehose sur un autre AWS compte. Cela nécessite de définir une destination et de configurer les autorisations appropriées dans les deux comptes.

Pour obtenir des instructions sur la configuration de la journalisation entre comptes, y compris les rôles et politiques IAM requis, consultez la section Configuration d'un nouvel abonnement multicompte dans le guide de l'utilisateur Amazon CloudWatch .

Envoi des journaux système du fournisseur de capacité à Amazon S3

Vous pouvez envoyer les journaux système du fournisseur de capacité à Amazon Simple Storage Service. Avec Amazon S3, vous pouvez stocker des journaux de manière rentable pour une conservation à long terme et les analyser à l'aide de services tels qu'Athena.

> **Note**
>
> Vous pouvez configurer les journaux système du fournisseur de capacité à envoyer à Amazon S3 à l'aide des AWS kits SDK et de tous les kits de développement logiciel. AWS CLI AWS CloudFormation

Tarification

Pour plus d'informations sur la tarification, consultez la page CloudWatch Tarification Amazon.

Configuration de la livraison des journaux Amazon S3

Pour envoyer les journaux système du fournisseur de capacité à Amazon S3, créez un filtre d'abonnement CloudWatch aux journaux dans le groupe de journaux de votre fournisseur de capacité. Le filtre d'abonnement achemine les événements du journal vers votre compartiment Amazon S3.

Par défaut, le groupe de journaux de votre fournisseur de capacité est nommé`/aws/lambda/capacity-provider/<capacity-provider-name>`. Utilisez ce groupe de journaux lors de la création du filtre d'abonnement.

Pour obtenir des instructions sur la configuration d'un filtre d'abonnement pour Amazon S3, y compris la création de rôles IAM et les autorisations de compartiment, consultezEnvoi des journaux des fonctions d'événements Lambda à Amazon S3.

Cross-account journalisation

Vous pouvez configurer votre fournisseur de capacité pour qu'il envoie des journaux à un compartiment Amazon S3 d'un autre AWS compte. Cela nécessite de définir une destination et de configurer les autorisations appropriées dans les deux comptes.

Pour obtenir des instructions sur la configuration de la journalisation entre comptes, y compris les rôles et politiques IAM requis, consultez la section Configuration d'un nouvel abonnement multicompte dans le guide de l'utilisateur Amazon CloudWatch .

Quotas d'instances gérées Lambda

Cette page décrit les quotas de service pour les instances gérées AWS Lambda. Ces quotas sont distincts des quotas AWS Lambda (par défaut). Certains quotas peuvent être augmentés sur demande.

Outre les quotas répertoriés sur cette page, les instances gérées Lambda sont soumises aux quotas de service Amazon EC2 appliqués à votre compte. Les quotas qui affectent généralement les clients des instances gérées Lambda incluent les limites de vCPU de type d'instance EC2, les limites de volume Amazon EBS et les adresses IP disponibles dans vos sous-réseaux VPC.

Quotas de demandes d'API Lambda

Ces quotas contrôlent le taux auquel vous pouvez effectuer des appels d'API pour gérer les fournisseurs de capacité des instances gérées Lambda. Les limites de débit des API de lecture et d'écriture s'appliquent à toutes les opérations des fournisseurs de capacité combinées, y compris la création, la mise à jour, la description et la suppression de fournisseurs de capacité.

Ressource	Quota
Le taux combiné maximal (demandes par seconde) pour toutes les API de lecture du fournisseur de capacité	15 requêtes par seconde. Il ne peut pas être augmenté.

Ressource	Quota
Le taux combiné maximal (demandes par seconde) pour toutes les API d'écriture du fournisseur de capacité	1 demande par seconde. Il ne peut pas être augmenté.

Quotas de ressources pour les instances gérées Lambda

Ces quotas définissent les limites des ressources principales des instances gérées Lambda au sein de votre AWS compte. Ils régissent le nombre de fournisseurs de capacité que vous pouvez créer et le nombre de versions de fonctions qui peuvent être associées à chaque fournisseur de capacité.

Ressource	Quota
Fournisseurs de capacité	1 000. Le nombre maximum de fournisseurs de capacité créés dans un compte.
Versions de fonctions par fournisseur de capacité	100. Le nombre maximum de versions de fonctions par fournisseur de capacité. Il ne peut pas être augmenté.
vCPU par fournisseur de capacité	15 000. Le nombre maximum de vCPU par fournisseur de capacité.

Quotas de mappage de la source

Ces quotas contrôlent le débit et les limites de configuration pour le traitement des événements provenant de divers AWS services sur les instances gérées Lambda. Les limites de débit garantissent des performances prévisibles, tandis que les limites du nombre de mappages contribuent à maintenir la stabilité du service. Les mappages de sources d'événements sur les instances gérées Lambda prennent en charge Amazon SQS, DynamoDB Streams, Amazon Kinesis Data Streams, Amazon MSK et Apache Kafka autogéré en tant que sources d'événements.

Ressource	Quota
Débit de mappage des sources d'événements SQS standard sur les instances gérées Lambda	5 Mo par seconde. Il ne peut pas être augmenté.
Débit de mappage des sources d'événements Kafka standard sur les instances gérées Lambda	1 Mo par seconde. Il ne peut pas être augmenté.
Mappages de sources d'événements Kafka standard sur les instances gérées Lambda	100 mappages de sources d'événements. Il ne peut pas être augmenté.
Débit de mappage des sources d'événements Kinesis sur les instances gérées Lambda	25 Mo par seconde. Peut être augmenté.
Débit de mappage des sources d'événements DynamoDB sur les instances gérées Lambda	10 Mo par seconde. Peut être augmenté.
Invoquer le débit des demandes pour les appels asynchrones sur les instances gérées Lambda	5 Mo par seconde. Peut être augmenté.

Demande d’augmentation de quota

Pour les quotas qui peuvent être augmentés, vous pouvez demander une augmentation via la console Service Quotas.

Pour demander une augmentation de quota

1. Ouvrez la console Service Quotas sur console.aws.amazon. com/servicequotas/.
2. Dans le panneau de navigation, choisissez Services AWS .
3. Choisissez AWS Lambda.
4. Sélectionnez le quota que vous souhaitez augmenter.
5. Choisissez Request quota increase (Demander une augmentation de quota).
6. Entrez la nouvelle valeur du quota et justifiez l'augmentation.
7. Cliquez sur Demander.

Étapes suivantes

- En savoir plus sur les fournisseurs de capacité pour les instances gérées Lambda
- Comprendre le dimensionnement pour les instances gérées Lambda
- Consultez les guides spécifiques à l'exécution pour Java et Node.jsPython
- Configurez la connectivité VPC pour vos fournisseurs de capacité

Bonnes pratiques pour les instances gérées Lambda

Configuration du fournisseur de capacité

Séparez les fournisseurs de capacité par niveau de confiance. Créez différents fournisseurs de capacité pour les charges de travail présentant des exigences de sécurité différentes. Toutes les fonctions d'événement Lambda attribuées au même fournisseur de capacité doivent être mutuellement fiables, car les fournisseurs de capacité servent de limite de sécurité.

Utilisez des noms descriptifs. Nommez les fournisseurs de capacité pour indiquer clairement leur utilisation prévue et leur niveau de confiance (par exemple`production-trusted`,`dev-sandbox`). Cela permet aux équipes de comprendre l'objectif et le niveau de sécurité de chaque fournisseur de capacité.

Utilisez plusieurs zones de disponibilité. Spécifiez des sous-réseaux dans plusieurs zones de disponibilité lors de la création de fournisseurs de capacité. Lambda lance trois instances par défaut pour la résilience AZ, garantissant ainsi la haute disponibilité de vos fonctions.

Sélection du type d'instance

Laissez Lambda choisir les types d'instances. Par défaut, Lambda choisit les types d'instances les mieux adaptés à votre charge de travail. Nous vous recommandons de laisser les instances gérées Lambda choisir les types d'instances à votre place, car la restriction du nombre de types d'instances possibles peut entraîner une baisse de disponibilité.

Spécifiez les types d'instances pour des besoins spécifiques. Si vous avez des exigences matérielles spécifiques, définissez les types d'instances autorisés dans une liste d'instances compatibles. Par exemple :

- Pour les applications nécessitant une bande passante réseau élevée, sélectionnez plusieurs types d'instances n

- Pour les environnements de test ou de développement soumis à des contraintes de coût, choisissez des types d'instances plus petits tels que m7a.large

Configuration de la fonction

Choisissez les paramètres de mémoire et de vCPU appropriés. Sélectionnez des configurations de mémoire et de vCPU qui prennent en charge les exécutions simultanées de votre fonction. La taille de fonction minimale prise en charge est de 2 Go et 1 vCPU.

- Pour les applications Python, choisissez un ratio mémoire/vCPU plus élevé (par exemple 4 pour 1 ou 8 pour 1) en raison de la façon dont Python gère la multisimultanéité
- Pour les CPU-intensive opérations ou les fonctions qui effectuent peu d'E/S, choisissez plusieurs vCPU
- Pour les IO-heavy applications telles que les services Web ou les tâches par lots, la multisimultanéité offre le plus d'avantages

Configurez la simultanéité maximale de manière appropriée. Lambda choisit des valeurs par défaut raisonnables pour une simultanéité maximale qui équilibre la consommation de ressources et le débit. Ajustez ce paramètre en fonction de l'utilisation des ressources de votre fonction :

- Augmentez la simultanéité maximale (jusqu'à 64 par vCPU) si vos invocations de fonctions utilisent très peu de CPU
- Diminuez la simultanéité maximale si votre application consomme une grande quantité de mémoire et très peu de processeur

Notez que les environnements d'exécution présentant une très faible simultanéité peuvent être confrontés à des ralentissements et à des difficultés de mise à l'échelle.

Long-running fonctions

Les fonctions des instances AWS Lambda gérées peuvent s'exécuter pendant 90 minutes (5 400 secondes) par appel pour les invocations asynchrones et pour les invocations de mappage des sources d'événements, à l'exception des mappages des sources d'événements Amazon MQ et Amazon DocumentDB, qui restent limités à 15 minutes. Les appels synchrones et la phase d'initialisation des fonctions restent également limités à 15 minutes. Pour plus d'informations sur la définition du délai d'expiration, voir Configurer le délai d'expiration de la fonction Lambda. Étant

donné que votre fonction peut s'exécuter plus longtemps, prenez en compte les considérations suivantes pour les composants de nature éphémère, tels que les connexions réseau et les informations d'identification.

Tenez compte des délais d'inactivité des connexions. Assurez-vous que les délais de connexion inactifs sur les services en aval tels qu'Amazon RDS ElastiCache, Amazon et les API externes tiennent compte de la durée complète des fonctions. Si votre fonction achemine le trafic via une passerelle NAT, envoyez des paquets keep-alive pour éviter que les connexions inactives ne soient abandonnées après le délai d'inactivité de 350 secondes de la passerelle NAT.

Respectez les valeurs TTL du DNS. Respectez les valeurs TTL du DNS lorsque vous résolvez des noms d'hôtes externes. Les AWS SDK gèrent cela automatiquement, mais les clients HTTP personnalisés peuvent mettre en cache des résolutions DNS au-delà de leur TTL.

Actualisez les informations d'identification temporaires. Si votre fonction acquiert des informations d'identification ou des jetons temporaires, vérifiez qu'ils restent valides pendant toute la durée d'exécution ou actualisez-les en arrière-plan.

Conception axée sur l'idempuissance. Lambda ne garantit pas un traitement en une seule fois. Au fur et à mesure que les fonctions s'allongent, la fenêtre de nouvelles tentatives et de doublons de livraisons augmente. Utilisez Powertools for AWS Lambda pour implémenter l'idempotencie pour des opérations telles que les paiements ou les écritures de base de données, afin qu'elles produisent le même résultat même si elles sont exécutées plusieurs fois. Si vous utilisez les fonctions durables Lambda, les étapes ont une sémantique d'exécution au moins une fois : le SDK d'exécution durable ignore les étapes terminées pendant la rediffusion, mais les étapes qui échouent avant le point de contrôle peuvent être exécutées à nouveau. Vous pouvez utiliser les noms d'exécution comme clés d'idempuissance.

Ajustez les mappages des sources d'événements pour un traitement plus long. Pour Amazon SQS, définissez le délai de visibilité de la file d'attente à au moins six fois le délai d'expiration de la fonction, afin que Lambda dispose de suffisamment de temps pour réessayer un lot si la fonction est limitée. Lambda valide cela lorsque vous créez le mappage des sources d'événements, mais n'empêche pas les modifications ultérieures de la file d'attente ou de la fonction qui créent une incompatibilité. Pour Amazon Kinesis Data Streams et Amazon DynamoDB Streams, configurez la fenêtre de traitement par lots maximale et le facteur de parallélisation afin de prendre en compte les délais de traitement plus longs par lot, et activez le signalement partiel des défaillances de lots afin que seuls les enregistrements ayant échoué soient réessayés au lieu du lot complet.

Configuration de la mise à l'échelle

Définissez une utilisation cible appropriée des ressources. Par défaut, Lambda conserve une marge de manœuvre suffisante pour que votre trafic double en 5 minutes sans limitation. Ajustez cela en fonction des caractéristiques de votre charge de travail :

- Pour des charges de travail très stables ou des applications non sensibles aux limitations, fixez l'objectif à un niveau élevé afin d'augmenter le taux d'utilisation et de réduire les coûts
- Pour les charges de travail susceptibles de générer des pics de trafic, définissez des objectifs de ressources à un niveau bas afin de conserver une marge de manœuvre supplémentaire

Planifiez la croissance du trafic. Si votre trafic double plus que dans les 5 minutes, vous risquez de constater des ralentissements à mesure que Lambda augmente le nombre d'instances et d'environnements d'exécution. Concevez votre application de manière à gérer les ralentissements potentiels pendant les périodes de mise à l'échelle rapide.

Sécurité

Appliquez le moindre privilège pour PassCapacityProvider les autorisations. N'accordez `lambda:PassCapacityProvider` des autorisations qu'aux fournisseurs de capacité nécessaires. Utilisez les autorisations au niveau des ressources pour limiter les fournisseurs de capacité que les utilisateurs peuvent affecter aux fonctions.

Surveillez l'utilisation des fournisseurs de capacité. AWS CloudTrail À utiliser pour surveiller les attributions des fournisseurs de capacité et les modèles d'accès. Cela permet d'identifier les tentatives d'accès non autorisées et de garantir le respect des politiques de sécurité.

Séparez les charges de travail non fiables. Ne vous fiez pas aux conteneurs pour isoler la sécurité entre les charges de travail non fiables. Utilisez différents fournisseurs de capacité pour séparer les charges de travail qui ne sont pas mutuellement fiables.

Optimisation des coûts

Utilisez les options de tarification EC2. Profitez des plans EC2 Savings Plans et des instances réservées pour réduire les coûts. Ces options de tarification s'appliquent au calcul EC2 sous-jacent (les frais de gestion de 15 % ne sont pas réduits).

Optimisez les charges de travail en régime permanent. Les instances gérées Lambda sont particulièrement adaptées aux fonctions en régime permanent avec un volume de trafic élevé prévisible. Pour les modèles de trafic en rafale, Lambda (par défaut) peut être plus rentable.

Surveillez l'utilisation des ressources. Suivez CloudWatch les métriques pour comprendre l'utilisation du processeur et de la mémoire. Ajustez l'allocation de mémoire des fonctions et la sélection du type d'instance en fonction des modèles d'utilisation réels afin d'optimiser les coûts.

Surveillance et observabilité

Surveillez les indicateurs des fournisseurs de capacité. Suivez les indicateurs au niveau des fournisseurs de capacité, MemoryUtilization notamment l'utilisation du processeur et la disponibilité de vCPUAvailable, et vérifiez que des ressources suffisantes sont disponibles MemoryAvailable pour vos charges de travail.

Surveillez les métriques de l'environnement d'exécution. Suivez les indicateurs au niveau de l'environnement d'exécution, notamment ExecutionEnvironmentConcurrency ExecutionEnvironmentConcurrencyLimit pour comprendre le comportement de dimensionnement et identifier les ralentissements potentiels.

Configurez des CloudWatch alarmes. Créez des CloudWatch alarmes pour les indicateurs clés afin d'identifier les problèmes de manière proactive :

- Utilisation élevée du processeur ou de la mémoire
- Faible capacité disponible
- À l'approche des limites de simultanéité

Language-specific considérations

Suivez les meilleures pratiques spécifiques à la langue. Chaque langage de programmation gère différemment la multisimultanéité. Consultez les guides spécifiques aux langues pour obtenir des recommandations détaillées :

- Java : utilisez des collections adaptées aux threads et `ThreadLocal` pour un état `AtomicInteger` spécifique à la demande
- Node.js: à utiliser InvokeStore pour tous les états spécifiques à la demande et éviter les variables globales

- Python : utilisez des noms de fichiers uniques `/tmp` avec les identifiants de demande et envisagez une isolation de la mémoire basée sur les processus
- Rust : À utiliser à la `run_concurrent` place de`run`, avec la `concurrency-tokio` fonctionnalité activée. Le gestionnaire doit être `Clone` `+Send`.

Testez les problèmes de sécurité et de simultanéité des threads. Avant le déploiement en production, testez soigneusement vos fonctions pour détecter les problèmes de sécurité des threads, les conditions de course et l'isolation correcte des états sous charge simultanée.

Étapes suivantes

- En savoir plus sur les fournisseurs de capacité pour les instances gérées Lambda
- Comprendre le dimensionnement pour les instances gérées Lambda
- Consultez les guides spécifiques à l'exécution pour Java et Node.jsPython
- Configurez la connectivité VPC pour vos fournisseurs de capacité
- Surveillez les instances gérées Lambda à l'aide de métriques CloudWatch

Résolution des problèmes liés aux instances gérées Lambda

Problèmes de limitation et de dimensionnement

étranglement occasionnel

Problème : vous rencontrez des erreurs d'étranglement (HTTP 429) pendant les opérations normales.

Cause : Les instances gérées Lambda peuvent rejeter les nouvelles invocations afin de protéger les appels déjà en cours. Si le taux d'utilisation de vos environnements d'exécution est constamment élevé, les nouvelles invocations peuvent être limitées.

Solution :

- Surveillez les indicateurs de dimensionnement : examinez le graphique des raisons de l'étranglement pour comprendre la raison des problèmes d'étranglement et de mise à l'échelle des capacités. Dans l'exemple suivant, un processeur trop élevé provoque des ralentissements.
- Vérifiez la configuration des fonctions : assurez-vous que la mémoire de vos fonctions et les paramètres du processeur virtuel prennent en charge les exécutions multisimultanées.

Augmentez la mémoire des fonctions ou l'allocation du processeur virtuel si nécessaire. S'il `ExecutionEnvironmentVCPUUtilization` est élevé, essayez d'ajouter plus de processeurs virtuels par fonction.

```
aws lambda update-function \
  --function-name my-function \
  ...
  --memory-size 8192
```

S'il `ExecutionEnvironmentMemoryUtilization` est élevé, essayez d'ajouter de la mémoire par processeur virtuel :

```
aws lambda update-function \
  --function-name my-function \
  --capacity-provider-config '{
    "LambdaManagedInstancesCapacityProviderConfig": {
      "ExecutionEnvironmentMemoryGiBPerVCpu": 4.0
    }
  }'
```

Accélérations lors de la mise à l'échelle

Problème : vous rencontrez des erreurs de limitation (HTTP 429) lorsque le trafic augmente rapidement.

Cause : Les instances gérées Lambda évoluent de manière asynchrone en fonction de l'utilisation des ressources du processeur et de la saturation multisimultanéité. Si votre trafic fait plus que doubler en 5 minutes, vous risquez de rencontrer des problèmes à mesure que Lambda fait évoluer les instances et les environnements d'exécution pour répondre à la demande.

Solutions :

- Ajustez l'utilisation des ressources cibles : si votre charge de travail présente des modèles de trafic prévisibles, définissez une utilisation des ressources cible plus faible afin de conserver une marge de manœuvre supplémentaire en cas de rafales de trafic.

```
aws lambda create-capacity-provider \
  --name my-capacity-provider \
  ...
  --capacity-provider-scaling-config '{
```

```
    "ScalingMode": "Manual",
    "ScalingPolicies": [
      {
        "PredefinedMetricType": "LambdaCapacityProviderAverageCPUUtilization",
        "TargetValue": 30.0
      }
    ]
  }'
```

- Pre-warm capacité : pour les augmentations de trafic planifiées, utilisez l'`PutFunctionScalingConfig`API pour préchauffer la capacité supplémentaire.

```
aws lambda put-function-scaling-config \
  --function-name my-function \
  --qualifier 1 \
  --function-scaling-config '{
    "MinExecutionEnvironments": 100
  }'
```

Réduction lente

Problème : les instances mettent beaucoup de temps à être réduites après une diminution du trafic.

Cause : Les instances gérées Lambda sont progressivement réduites pour maintenir la disponibilité et éviter les changements de capacité rapides qui pourraient avoir un impact sur les performances.

Solution :

Ce comportement est normal. Lambda réduit les instances de manière conservatrice pour garantir la stabilité. Surveillez vos CloudWatch statistiques pour suivre le nombre d'instances en cours d'exécution.

Problèmes de simultanéité

Environnements d'exécution avec de faibles limites d'expérience de simultanéité

Problème : Vos fonctions sont ralenties malgré la disponibilité de la capacité.

Cause : Les environnements d'exécution dont la simultanéité maximale est très faible peuvent avoir des difficultés à évoluer efficacement. Les instances gérées Lambda sont conçues pour les applications multisimultanées.

Solutions :

- Augmentez la simultanéité maximale : si les invocations de vos fonctions utilisent très peu de processeur, augmentez le paramètre de simultanéité maximale à 64 par processeur virtuel.

```
aws lambda update-function \
  --function-name ordering-api-backend \
  --capacity-provider-config '{
    "LambdaManagedInstancesCapacityProviderConfig": {
      "PerExecutionEnvironmentMaxConcurrency": 32
    }
  }'
```

- Optimisez le code de fonction : révisez votre code de fonction pour réduire la consommation du processeur par appel, ce qui permet une plus grande simultanéité.
- Réglez la mémoire des fonctions et le processeur virtuel : assurez-vous que votre fonction dispose de suffisamment de ressources pour gérer plusieurs appels simultanés.

Problèmes de sécurité des threads (environnement d'exécution Java)

Problème : Votre fonction Java produit des résultats incorrects ou se heurte à des conditions de concurrence lorsqu'elle est chargée.

Cause : plusieurs threads exécutent la méthode du gestionnaire simultanément et l'état partagé n'est pas sécurisé pour les threads.

Solution :

- Utilisez `AtomicInteger` ou `AtomicLong` pour les compteurs au lieu de types primitifs
- Remplacez `HashMap` par `ConcurrentHashMap`.
- Utiliser `Collections.synchronizedList()` pour emballer `ArrayList`
- À utiliser `ThreadLocal` pour un état spécifique à la demande
- Accédez aux ID de trace depuis l'objet Lambda Context, et non depuis les variables d'environnement

Pour obtenir des conseils détaillés, consultez la documentation relative à l'environnement d'exécution Java pour les instances gérées Lambda.

Problèmes d'isolation des états (Node.js exécution)

Problème : votre Node.js fonction renvoie des données provenant de différentes requêtes ou est corrompue.

Cause : Les variables globales sont partagées lors d'appels simultanés sur le même thread de travail. Lorsque les opérations asynchrones permettent de contrôler, d'autres invocations peuvent modifier l'état partagé.

Solution :

- Installation et utilisation `@aws/lambda-invoke-store` pour tous les états spécifiques à la demande
- Remplacez les variables globales par `InvokeStore.set()` et `InvokeStore.get()`
- Utiliser des noms de fichiers uniques dans `/tmp` les ID de demande
- Accédez aux ID de trace en utilisant `InvokeStore.getXRayTraceId()` plutôt des variables d'environnement

Pour obtenir des conseils détaillés, consultez la documentation relative à l'Node.js environnement d'exécution pour les instances gérées Lambda.

Conflits de fichiers (environnement d'exécution Python)

Problème : Votre fonction Python lit des données incorrectes à partir de fichiers au format`/tmp`.

Cause : plusieurs processus partagent le `/tmp` répertoire. Les écritures simultanées dans le même fichier peuvent entraîner une corruption des données.

Solution :

- Utilisez des noms de fichiers uniques avec des ID de demande : `/tmp/request_{context.request_id}.txt`
- Utiliser le verrouillage des fichiers avec `fcntl.flock()` pour les fichiers partagés
- Nettoyez les fichiers temporaires avec `os.remove()` After Use

Pour obtenir des conseils détaillés, consultez la documentation relative à l'environnement d'exécution Python pour les instances gérées Lambda.

Problèmes de performance

Utilisation élevée de la mémoire

Problème : Vos fonctions présentent une forte utilisation de la mémoire ou des erreurs de mémoire insuffisante.

Cause : Chaque requête simultanée en Python s'exécute dans un processus distinct avec son propre espace mémoire. L'utilisation totale de la mémoire est égale à la mémoire par processus multipliée par les processus simultanés.

Solution :

- Surveillez la `MemoryUtilization` métrique dans CloudWatch
- Réduisez le `MaxConcurrency` réglage si l'utilisation de la mémoire approche de la limite de mémoire de la fonction
- Augmenter l'allocation de mémoire des fonctions pour permettre une plus grande simultanéité
- Optimisez l'utilisation de la mémoire en chargeant les données à la demande plutôt que pendant l'initialisation

Des performances incohérentes

Problème : les performances des fonctions varient considérablement d'une invocation à l'autre.

Cause : Lambda peut sélectionner différents types d'instances en fonction de la disponibilité, ou des fonctions peuvent être exécutées sur des instances dont la disponibilité des ressources varie.

Solution :

- Spécifiez les types d'instances autorisés : si vous avez des exigences de performances spécifiques, configurez les types d'instances autorisés dans votre fournisseur de capacité afin de limiter les types d'instances que Lambda peut sélectionner.
- Surveillez les indicateurs au niveau de l'instance : effectuez un suivi `CPUUtilization` et `MemoryUtilization` au niveau du fournisseur de capacité pour identifier les contraintes en matière de ressources.
- Passez en revue les indicateurs de capacité : vérifiez `vCPUAvailable` et `MemoryAvailable` assurez-vous que des ressources suffisantes sont disponibles sur vos instances.

Problèmes liés aux fournisseurs de capacités

La version de la fonction ne devient pas ACTIVE

Problème : la version de votre fonction reste en attente après la publication.

Cause : Lambda lance des instances gérées et démarre des environnements d'exécution. Ce processus prend du temps, en particulier pour la première version de fonction sur un nouveau fournisseur de capacité.

Solution :

Attendez que Lambda termine le processus d'initialisation. Lambda lance trois instances par défaut pour la résilience AZ et démarre trois environnements d'exécution avant de marquer la version de votre fonction comme ACTIVE. Cela prend généralement plusieurs minutes.

Impossible de supprimer le fournisseur de capacité

Problème : un message d'erreur s'affiche lorsque vous tentez de supprimer un fournisseur de capacité.

Cause : Vous ne pouvez pas supprimer un fournisseur de capacité auquel sont associées des versions de fonctions.

Solution :

1. Identifiez toutes les versions de fonctions à l'aide du fournisseur de capacité à l'aide de l'`ListFunctionVersionsByCapacityProvider`API.
2. Supprimez ou mettez à jour ces versions de fonctions pour supprimer l'association de fournisseur de capacité.
3. Réessayez de supprimer le fournisseur de capacité.

Messages d'erreur génériques lors de la publication des fonctions

Problème : vous rencontrez des messages d'erreur génériques tels que « Une erreur interne s'est produite lors de la publication » lors de la publication des fonctions.

Solution :

- Vérifiez les autorisations IAM : assurez-vous de disposer de l'`lambda:PassCapacityProvider`autorisation pour le fournisseur de capacité que vous essayez d'utiliser.
- Vérifiez la configuration du fournisseur de capacité : confirmez que votre fournisseur de capacité est à l'état ACTIF à l'aide de l'`GetCapacityProvider`API.
- Vérifiez la configuration du VPC : assurez-vous que les sous-réseaux et les groupes de sécurité spécifiés dans votre fournisseur de capacité sont correctement configurés et accessibles.
- Vérifiez les AWS CloudTrail journaux : consultez CloudTrail les journaux pour obtenir des informations détaillées sur les erreurs relatives à l'échec de l'opération.

Problèmes de surveillance et d'observabilité

CloudWatch Métriques manquantes

Problème : vous ne voyez pas les mesures attendues CloudWatch pour votre fournisseur de capacité ou vos fonctions.

Cause : Les métriques sont publiées à intervalles d'une minute. Les nouveaux fournisseurs de capacité ou les nouvelles fonctions peuvent ne pas disposer de métriques immédiatement.

Solution :

Attendez au moins 5 à 10 minutes après la publication d'une version de fonction avant de vous attendre à ce que les métriques apparaissent dans CloudWatch. Vérifiez que vous recherchez l'espace de noms (`AWS/Lambda`) et les dimensions (`CapacityProviderName`FunctionName, ou`InstanceType`) corrects.

Impossible de trouver les CloudWatch journaux

Problème : Votre fonction s'exécute correctement, mais vous ne trouvez pas de journaux dans les CloudWatch journaux.

Cause : Les instances gérées Lambda s'exécutent dans votre VPC et nécessitent une connectivité réseau pour envoyer des journaux à CloudWatch Logs. Sans configuration de connectivité VPC appropriée, vos fonctions ne peuvent pas atteindre le point de terminaison du service CloudWatch Logs.

Solution :

Configurez la connectivité VPC pour permettre à vos fonctions d'envoyer des CloudWatch journaux à Logs. Trois possibilités s'offrent à vous :

Option 1 : point de terminaison VPC pour les CloudWatch journaux (recommandé pour la production)

1. Ouvrez la console Amazon VPC à l'adresse console.aws.amazon. com/vpc/.
2. Dans le panneau de navigation, choisissez Points de terminaison.
3. Choisissez Créer un point de terminaison.
4. Pour Service category (Catégorie de service), choisissez Services AWS .
5. Dans le champ Nom du service, sélectionnez `com.amazonaws.region.logs` (remplacez `region` par votre AWS région).
6. Pour VPC, sélectionnez le VPC utilisé par votre fournisseur de capacité.
7. Pour Sous-réseaux, sélectionnez les sous-réseaux dans lesquels vous souhaitez créer des interfaces réseau de terminaux. Pour assurer la haute disponibilité, sélectionnez les sous-réseaux dans plusieurs zones de disponibilité.
8. Pour les groupes de sécurité, sélectionnez les groupes de sécurité qui autorisent le trafic HTTPS entrant (port 443) à partir du groupe de sécurité de votre fonction.
9. Activez le DNS privé pour le terminal.
10. Choisissez Créer un point de terminaison.

Option 2 : sous-réseau public avec passerelle Internet

Si votre fournisseur de capacité utilise des sous-réseaux publics, assurez-vous que :

1. Une passerelle Internet est connectée à votre VPC
2. La table de routage achemine le `0.0.0.0/0` trafic vers la passerelle Internet
3. Les groupes de sécurité autorisent le trafic HTTPS sortant sur le port 443

Option 3 : sous-réseau privé avec passerelle NAT

Si votre fournisseur de capacité utilise des sous-réseaux privés, assurez-vous que :

1. Une passerelle NAT existe dans un sous-réseau public
2. La table de routage du sous-réseau privé achemine le `0.0.0.0/0` trafic vers la passerelle NAT
3. La table de routage des sous-réseaux publics achemine `0.0.0.0/0` le trafic vers une passerelle Internet

4. Les groupes de sécurité autorisent le trafic HTTPS sortant sur le port 443

Pour obtenir des conseils détaillés sur les options de connectivité VPC, consultez la section Connectivité VPC pour les instances gérées Lambda.

Difficulté à corréler les journaux des demandes simultanées

Problème : les journaux des différentes demandes sont entrelacés, ce qui rend difficile le suivi des demandes individuelles.

Cause : L'entrelacement des journaux est un comportement normal et normal dans les systèmes multisimultanés.

Solution :

- Utilisez la journalisation structurée au format JSON : incluez l'ID de demande dans toutes les instructions de journal
- Java : utilisez Log4j avec `ThreadContext` pour inclure automatiquement l'ID de demande
- Node.js: à utiliser `console.log()` avec le formatage JSON et à inclure `InvokeStore.getRequestId()`
- Python : utilisez le module de journalisation standard au format JSON et incluez `context.request_id`

Pour obtenir des conseils détaillés, consultez les pages de documentation spécifiques à l'exécution.

Aide supplémentaire

Si les problèmes persistent après avoir essayé ces solutions :

1. Analysez CloudWatch les métriques : vérifiez les métriques du fournisseur de capacité et de l'environnement d'exécution pour identifier les contraintes en matière de ressources ou les problèmes de dimensionnement.
2. Consultez AWS CloudTrail les journaux : consultez CloudTrail les journaux pour obtenir des informations détaillées sur les appels d'API et les erreurs.
3. Contacter le AWS support : si vous ne parvenez pas à résoudre le problème, contactez le AWS support en fournissant des informations sur la configuration de votre fournisseur de capacité, la configuration des fonctions et les messages d'erreur spécifiques que vous rencontrez.

Étapes suivantes

- En savoir plus sur les fournisseurs de capacité pour les instances gérées Lambda
- Comprendre la mise à l'échelle pour les instances gérées Lambda
- Consultez les guides spécifiques à l'exécution pour Java et Node.js Python ???
- Surveillez les instances gérées Lambda à l'aide de métriques CloudWatch
- Passez en revue les meilleures pratiques pour les instances gérées Lambda

Gestion des dépendances des fonctions d'événement Lambda à l'aide de couches

Une couche Lambda est une archive de fichier .zip qui contient du code ou des données supplémentaires. Les couches contiennent généralement des dépendances de bibliothèque, une exécution personnalisée, ou des fichiers de configuration.

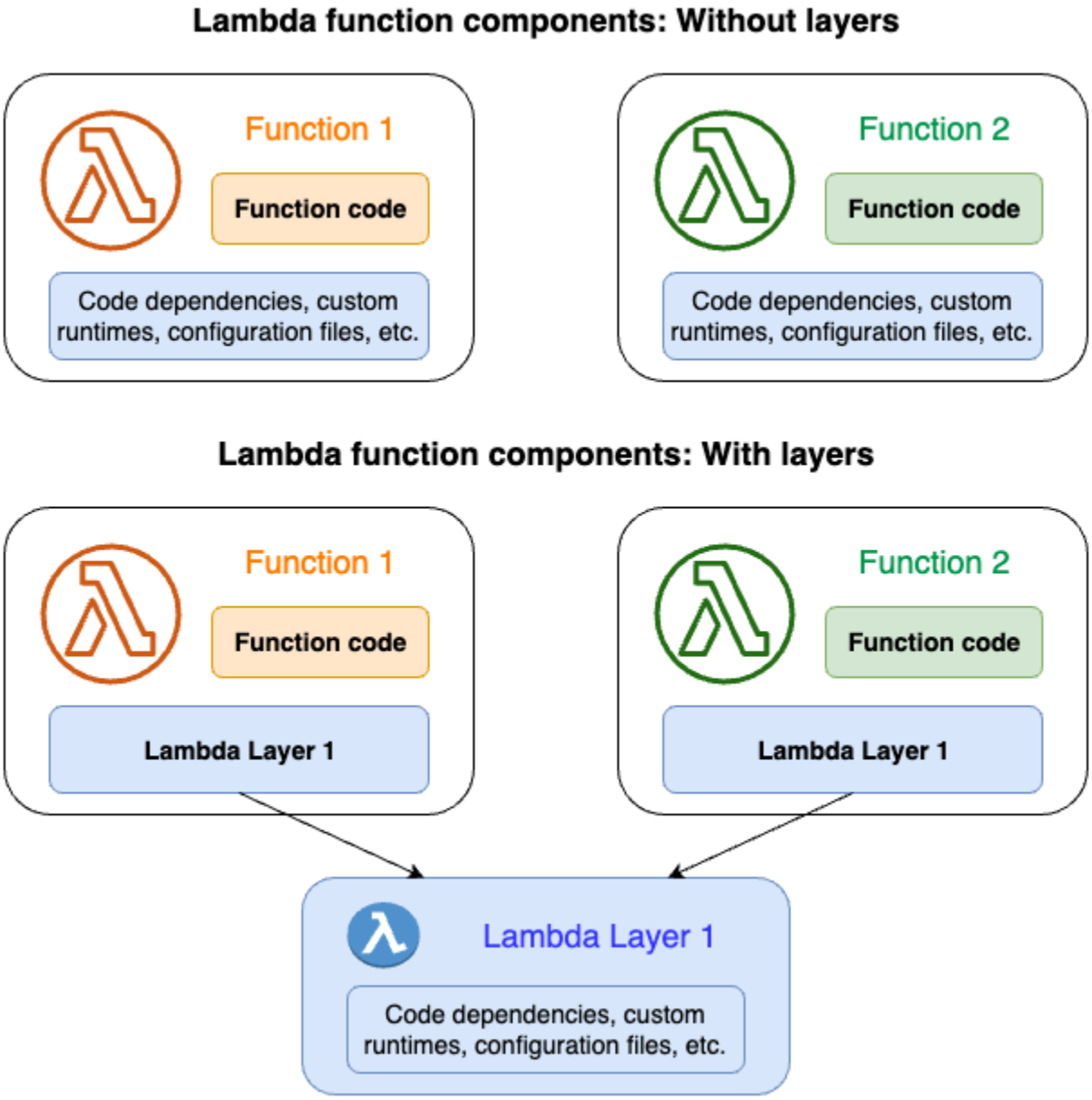
Vous pouvez envisager d'utiliser des couches pour plusieurs raisons :

- Pour réduire la taille de vos packages de déploiement. Au lieu d'inclure toutes les dépendances de votre fonction d'événement ainsi que le code de votre fonction d'événement dans votre package de déploiement, placez-les dans une couche. Cela permet de maintenir la taille et l'organisation des packages de déploiement.
- Pour séparer la logique des fonctions de base des dépendances. Avec les couches, vous pouvez mettre à jour les dépendances de votre fonction d'événement indépendamment du code de votre fonction d'événement, et vice versa. Cela favorise la séparation des préoccupations et vous aide à vous concentrer sur la logique de votre fonction événementielle.
- Pour partager les dépendances entre plusieurs fonctions. Après avoir créé une couche, vous pouvez l'appliquer à n'importe quel nombre de fonctions événementielles de votre compte. Sans couches, vous devez inclure les mêmes dépendances dans chaque package de déploiement individuel.
- Pour utiliser l'éditeur de code de la console Lambda. L'éditeur de code est un outil utile pour tester rapidement les mises à jour mineures du code Event Function. Toutefois, vous ne pouvez pas utiliser l'éditeur si la taille de votre package de déploiement est trop importante. L'utilisation de couches réduit la taille de votre package et peut débloquer l'utilisation de l'éditeur de code.
- Pour verrouiller une version du SDK intégré. Les SDK intégrés peuvent être modifiés sans préavis au fur et à mesure de la AWS sortie de nouveaux services et fonctionnalités. Vous pouvez

verrouiller une version du kit SDK en créant une couche Lambda avec la version spécifique requise. La fonction d'événement utilise alors toujours la version de la couche, même si la version intégrée au service change.

Si vous utilisez des fonctions d'événement Lambda dans Go ou Rust, nous vous déconseillons d'utiliser des couches. Pour les fonctions d'événement Go et Rust, vous fournissez le code de votre fonction d'événement sous forme d'exécutable, qui inclut votre code de fonction d'événement compilé ainsi que toutes ses dépendances. Le fait de placer vos dépendances dans une couche oblige votre fonction d'événement à charger manuellement des assemblages supplémentaires pendant la phase d'initialisation, ce qui peut augmenter les temps de démarrage à froid. Pour des performances optimales pour Go et Rust Event Functions, incluez vos dépendances dans votre package de déploiement.

Le schéma suivant illustre les différences architecturales de haut niveau entre deux fonctions d'événement qui partagent des dépendances. L'un utilise des couches Lambda, l'autre non.



Lorsque vous ajoutez une couche à une fonction d'événement, Lambda extrait le contenu de la couche dans le `/opt` répertoire de l'environnement d'exécution de votre fonction d'événement. Toutes les exécutions Lambda prises en charge en mode natif incluent des chemins vers des répertoires spécifiques dans le répertoire `/opt`. Cela permet à votre fonction d'événement d'accéder au contenu de votre couche. Pour plus d'informations sur ces chemins spécifiques et sur la manière d'empaqueter correctement vos couches, consultez the section called “Empaquetage des couches”.

Vous pouvez inclure jusqu'à cinq couches par fonction d'événement. Vous pouvez également utiliser des couches uniquement avec des fonctions d'événement Lambda déployées sous forme

d'archive de fichiers .zip. Pour les fonctions d'événement définies comme une image de conteneur, empaquetez votre environnement d'exécution préféré et toutes les dépendances du code lorsque vous créez l'image de conteneur. Pour plus d'informations, consultez la section Utilisation de couches et d'extensions Lambda dans des images de conteneur sur le blog AWS Compute.

Rubriques

- Utilisation des couches
- Couches et versions de couches
- Empaquetage du contenu de votre couche
- Création et suppression de couches dans Lambda
- Ajouter des couches aux fonctions événementielles
- Utilisation AWS CloudFormation avec couches
- Utilisation AWS SAM avec couches

Utilisation des couches

Pour créer une couche, empaquetez vos dépendances dans un fichier .zip, de la même manière que vous créer un package de déploiement normal. Plus précisément, le processus général de création et d'utilisation de couches comporte les trois étapes suivantes :

- Empaquetez d'abord le contenu de votre couche. Cela implique de créer une archive de fichiers .zip. Pour plus d'informations, consultez the section called “Empaquetage des couches”.
- Créez ensuite la couche dans Lambda. Pour plus d'informations, consultez the section called “Création et suppression de couches”.
- Ajoutez la couche à vos fonctions d'événement. Pour plus d'informations, consultez the section called “Ajout de couches”.

Couches et versions de couches

Une version de couche est un instantané immuable d'une version spécifique d'une couche. Lorsque vous créez une nouvelle couche, Lambda crée une nouvelle version de couche avec un numéro de version de 1. Chaque fois que vous publiez une mise à jour de la couche, Lambda incrémente le numéro de version et crée une nouvelle version de couche.

Chaque version de couche est identifiée par un Amazon Resource Name (ARN) unique. Lorsque vous ajoutez une couche à la fonction d'événement, vous devez spécifier la version de couche exacte que vous souhaitez utiliser (par exemple,`arn:aws:lambda:us-east-1:123456789012:layer:my-layer:1`).

Empaquetage du contenu de votre couche

Une couche Lambda est une archive de fichier .zip qui contient du code ou des données supplémentaires. Les couches contiennent généralement des dépendances de bibliothèque, une exécution personnalisée, ou des fichiers de configuration.

Cette section explique comment empaqueter correctement le contenu de votre couche. Pour plus d'informations conceptuelles sur les couches et les raisons pour lesquelles vous pourriez envisager de les utiliser, consultez the section called "Layers".

La première étape de la création d'une couche consiste à regrouper l'ensemble du contenu de la couche dans une archive de fichiers .zip. Parce que les fonctions Lambda s'exécutent sur Amazon Linux, le contenu de votre couche doit pouvoir être compilé et construit dans un environnement Linux.

Pour vous assurer que le contenu de votre couche fonctionne correctement dans un environnement Linux, nous vous recommandons de créer le contenu de votre couche à l'aide d'un outil comme Docker.

Rubriques

- Chemins d'accès de couche pour chaque exécution Lambda

Chemins d'accès de couche pour chaque exécution Lambda

Lorsque vous ajoutez une couche à une fonction, Lambda charge le contenu de la couche dans le répertoire `/opt` de cet environnement d'exécution. Pour chaque exécution Lambda, la variable `PATH` inclut déjà des chemins de dossiers spécifiques dans le répertoire `/opt`. Pour garantir que Lambda capture le contenu de votre couche, le fichier .zip de votre couche doit avoir ses dépendances un des chemins de dossier suivants :

Runtime	Chemin
Node.js	`nodejs/node_modules`
	`nodejs/node18/node_modules` (`NODE_PATH`)
	`nodejs/node20/node_modules` (`NODE_PATH`)
	`nodejs/node22/node_modules` (`NODE_PATH`)

Runtime	Chemin
Python	`python`
	`python/lib/ python3.x /site-packages` (répertoires de site)
Java	`java/lib` (`CLASSPATH`)
Ruby	`ruby/gems/3.4.0` (`GEM_PATH`)
	`ruby/lib` (`RUBYLIB`)
Toutes les exécutions	`bin` (`PATH`)
	`lib` (`LD_LIBRARY_PATH`)

Les exemples suivants montrent comment structurer les dossiers dans votre couche d'archive .zip.

Node.js

Example structure de fichier pour AWS X-Ray SDK pour Node.js

```
xray-sdk.zip
# nodejs/node_modules/aws-xray-sdk
```

Python

Example

```
python/              # Required top-level directory
### requests/
### boto3/
### numpy/
### (dependencies of the other packages)
```

Ruby

Example structure de fichiers pour la gem JSON

```
json.zip
```

```
# ruby/gems/3.4.0/
                | build_info
                | cache
                | doc
                | extensions
                | gems
                | # json-2.1.0
                # specifications
                  # json-2.1.0.gemspec
```

Java

Example structure de fichiers pour le fichier JAR Jackson

```
layer_content.zip
# java
    # lib
        # jackson-core-2.17.0.jar
        # <other potential dependencies>
        # ...
```

All

Example structure de fichiers pour la bibliothèque jq

```
jq.zip
# bin/jq
```

Pour obtenir des instructions spécifiques au langage et relatives à l'empaquetage, à la création et à l'ajout d'une couche, reportez-vous aux pages suivantes :

- Node.js – the section called "Layers"
- Python : the section called "Layers"
- Ruby – the section called "Layers"
- Java : the section called "Layers"

Nous vous déconseillons d'utiliser des couches pour gérer les dépendances des fonctions d'événement Lambda écrites en Go et Rust. Cela est dû au fait que les fonctions d'événement Lambda écrites dans ces langages se compilent en un seul exécutable, que vous fournissez à

Lambda lorsque vous déployez votre fonction d'événement. Cet exécutable contient le code de votre fonction d'événement compilé, ainsi que toutes ses dépendances. L'utilisation de couches complique non seulement ce processus, mais entraîne également une augmentation des temps de démarrage à froid, car vos fonctions événementielles doivent charger manuellement des assemblages supplémentaires en mémoire pendant la phase d'initialisation.

Pour utiliser des dépendances externes avec Go et Rust Lambda Event Functions, incluez-les directement dans votre package de déploiement.

Création et suppression de couches dans Lambda

Une couche Lambda est une archive de fichier .zip qui contient du code ou des données supplémentaires. Les couches contiennent généralement des dépendances de bibliothèque, une exécution personnalisée, ou des fichiers de configuration.

Cette section explique comment créer et supprimer des couches dans Lambda. Pour plus d'informations conceptuelles sur les couches et les raisons pour lesquelles vous pourriez envisager de les utiliser, consultez the section called "Layers".

Après avoir empaqueté le contenu de votre couche, l'étape suivante consiste à créer la couche dans Lambda. Cette section explique comment créer et supprimer des couches à l'aide de la console Lambda ou de l'API Lambda uniquement. Pour créer une couche à l'aide d' AWS CloudFormation, consultez the section called "Couches avec CloudFormation". Pour créer une couche à l'aide d' AWS Serverless Application Model (AWS SAM), consultez the section called "Couches avec AWS SAM".

Rubriques

- Création d'une couche
- Suppression d'une version de couche

Création d'une couche

Pour créer une couche, vous pouvez soit charger l'archive du fichier .zip depuis votre ordinateur local, soit depuis Amazon Simple Storage Service (Amazon S3). Lors du téléchargement depuis Amazon S3, vous pouvez choisir si Lambda copie le code Lambda-managed vers le stockage ou le référence directement depuis votre compartiment S3. Pour plus d'informations, consultez the section called "Self-managed Stockage de code S3".

Lambda extrait le contenu de la couche dans le `/opt` répertoire lors de la configuration de l'environnement d'exécution de la fonction d'événement Lambda.

Les couches peuvent avoir une ou plusieurs versions de couche. Lorsque vous créez une couche, Lambda définit la version de la couche sur version 1. Vous pouvez modifier les autorisations sur une version de couche existante à tout moment. Toutefois, pour mettre à jour le code ou apporter d'autres modifications de configuration, vous devez créer une nouvelle version de la couche.

Pour créer une couche (console)

1. Ouvrez la page Couches de la console Lambda.

2. Sélectionnez Créer un calque.
3. Sous Configuration de la couche, dans Nom, nommez votre couche.
4. (Facultatif) Dans le champ Description, saisissez une description pour le calque.
5. Pour télécharger le code de votre couche, effectuez l'une des opérations suivantes :
   - Pour charger un fichier .zip à partir de votre ordinateur, choisissez Charger un fichier .zip. Puis, sélectionnez Charger pour sélectionner votre fichier .zip local.
   - Pour charger un fichier à partir d'Amazon S3, choisissez Charger un fichier à partir d'Amazon S3. Ensuite, pour l'URL du lien Amazon S3, saisissez un lien vers le fichier.
6. Si vous avez choisi de télécharger depuis Amazon S3, sous Mode de stockage de code, choisissez l'une des options suivantes :
   - Mode de copie (par défaut)
   - Mode de référence
7. (Facultatif) Pour Architectures compatibles, choisissez une valeur ou les deux valeurs. Pour plus d'informations, consultez the section called "Kits d'instructions (ARM/x86)".
8. (Facultatif) Pour Exécutions compatibles, choisissez les exécutions avec lesquelles votre couche est compatible.
9. (Facultatif) Pour Licence, saisissez toutes les informations de licence nécessaires.
10. Cliquez sur Créer.

Vous pouvez également exécuter la commande publish-layer-version AWS Command Line Interface (CLI). Lors du téléchargement depuis Amazon S3, incluez-le `S3ObjectStorageMode=REFERENCE` pour utiliser le stockage de code S3 autogéré, ou omettez-le (par défaut`COPY`) pour utiliser le stockage. Lambda-managed Exemple :

```
aws lambda publish-layer-version --layer-name my-layer --zip-file fileb://layer.zip --
compatible-runtimes python3.14
```

Chaque fois que vous exécutez `publish-layer-version`, Lambda crée une nouvelle version de la couche.

Suppression d’une version de couche

Pour supprimer une version de couche, utilisez l'opération DeleteLayerVersionAPI. Par exemple, exécutez la AWS CLI commande delete-layer-version avec le nom de couche et la version de couche spécifiés.

```
aws lambda delete-layer-version --layer-name my-layer --version-number 1
```

Lorsque vous supprimez une version de couche, vous ne pouvez plus configurer de nouvelles fonctions d'événement pour l'utiliser. Cependant, toute fonction d'événement qui fait déjà référence à la version de couche supprimée continue de s'exécuter avec le contenu de cette couche. Lambda ne réutilise jamais les numéros de version pour le nom d'une couche.

Impact de la suppression de couches sur le quota de stockage

L'impact sur le quota de stockage de la suppression d'une version de couche dépend du mode de stockage utilisé par la couche et des fonctions qui la référencent.

La couche utilise Lambda-managed le stockage (COPY)

> Lorsque vous supprimez une version de couche qui utilise le Lambda-managed stockage, le code de couche est supprimé du quota de Lambda-managed stockage de votre compte. Cependant, toute fonction d'événement qui fait toujours référence à la version de couche supprimée continue d'avoir accès au contenu de la couche. Le contenu de la couche est pris en compte dans le quota de taille du package de déploiement de la fonction événementielle (250 Mo décompressés) mais n'est plus pris en compte dans le quota de stockage au niveau du compte. Lambda-managed

La couche utilise un stockage S3 autogéré (RÉFÉRENCE)

> Les couches qui utilisent le stockage de code S3 autogéré ne consomment pas d' Lambda-managed espace de stockage. Leur suppression n'a donc aucune incidence sur votre quota Lambda-managed de stockage. Les fonctions événementielles qui font référence à une version de couche autogérée supprimée continuent de s'exécuter normalement. Toutefois, si vous supprimez également l'objet source de votre compartiment S3 ou si vous révoquez l'accès de Lambda à celui-ci, vous ne pouvez plus mettre à jour la configuration de la fonction d'événement avec cette couche.

> **Note**
>
> La suppression d'une version de couche ne désactive jamais les fonctions d'événement qui y font référence. Les fonctions d'événement sont `Active` conservées, que la couche soit utilisée Lambda-managed ou que le stockage S3 soit autogéré. L'`Inactive`état ne s'applique que lorsque Lambda perd l'accès au code source d'une fonction d'événement stocké dans un compartiment S3 autogéré.

Ajouter des couches aux fonctions événementielles

Une couche Lambda est une archive de fichier .zip qui contient du code ou des données supplémentaires. Les couches contiennent généralement des dépendances de bibliothèque, une exécution personnalisée, ou des fichiers de configuration.

Cette section explique comment ajouter une couche à une fonction d'événement Lambda. Pour plus d'informations conceptuelles sur les couches et les raisons pour lesquelles vous pourriez envisager de les utiliser, consultez the section called "Layers".

Avant de configurer une fonction d'événement pour utiliser une couche, vous devez :

- Empaqueter le contenu de votre couche
- Créer une couche dans Lambda
- Assurez-vous que vous êtes autorisé à appeler l'GetLayerVersionAPI sur la version de la couche. Pour les fonctions événementielles de votre Compte AWS, vous devez disposer de cette autorisation dans votre politique utilisateur. Pour utiliser une couche dans un autre compte, le propriétaire de ce compte doit accorder l'autorisation à votre compte dans une stratégie basée sur les ressources. Pour obtenir des exemples, consultez the section called "Accès de la couche pour les autres comptes".

Vous pouvez ajouter jusqu'à cinq couches à une fonction d'événement. La taille totale décompressée de la fonction d'événement et de toutes les couches ne peut pas dépasser le quota de taille du package de déploiement décompressé de 250 Mo. Pour plus d'informations, consultez Quotas Lambda.

Vos fonctions événementielles peuvent continuer à utiliser n'importe quelle version de couche que vous avez déjà ajoutée, même après la suppression de cette version de couche ou après la révocation de votre autorisation d'accès à la couche. Cependant, vous ne pouvez pas créer une nouvelle fonction d'événement qui utilise une version de couche supprimée.

Pour ajouter une couche à une fonction d'événement

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez la fonction d'événement.
3. Faites défiler jusqu'à la section Couches, puis choisissez Ajouter une couche.
4. Sous Choisir une couche, choisissez une source de couche :

a. AWS couches : choisissez dans la liste des extensions AWS gérées.

b. Couches personnalisées : choisissez une couche créée dans votre Compte AWS.

c. Spécifiez un ARN : pour utiliser une couche provenant d'une autre couche Compte AWS, telle qu'une extension tierce, entrez le Amazon Resource Name (ARN).

5. Choisissez Ajouter.

L'ordre dans lequel vous ajoutez les couches correspond à l'ordre dans lequel Lambda fusionne ultérieurement le contenu de la couche dans l'environnement d'exécution. Vous pouvez modifier l'ordre de fusion des couches à l'aide de la console.

Pour mettre à jour l'ordre de fusion des couches pour votre fonction d'événement (console)

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez la fonction d'événement à configurer.
3. Sous Layers (Couches), choisissez Edit (Modifier).
4. Choisissez l'une des couches.
5. Choisissez Merge earlier (Fusionner plus tôt) ou Merge later (Fusionner plus tard) pour ajuster l'ordre des couches.
6. Cliquez sur Enregistrer.

Les couches sont versionnées. Le contenu de chaque version de couche est immuable. Le propriétaire d'une couche peut publier une nouvelle version de la couche pour fournir du contenu mis à jour. Vous pouvez utiliser la console pour mettre à jour la version de couche attachée à vos fonctions d'événement.

Pour mettre à jour les versions des couches pour votre fonction d'événement (console)

1. Ouvrez la page Couches de la console Lambda.
2. Choisissez la couche pour laquelle vous voulez mettre à jour la version.
3. Choisissez l'onglet Fonctions utilisant cette version.
4. Choisissez les fonctions d'événement que vous souhaitez modifier, puis choisissez Modifier.
5. Pour Version de la couche, choisissez la version de la couche à modifier.
6. Choisissez Update functions (Mettre à jour les fonctions).

Vous ne pouvez pas mettre à jour les versions de la couche Event Function entre AWS les comptes.

Recherche d'informations sur la couche

Pour trouver dans votre compte des couches compatibles avec le runtime de votre fonction d'événement, utilisez l'ListLayersAPI. Par exemple, vous pouvez utiliser la commande list-layers (AWS Command Line Interface CLI) suivante :

```
aws lambda list-layers --compatible-runtime python3.14
```

Vous devez voir des résultats similaires à ce qui suit :

```
{
    "Layers": [
        {
            "LayerName": "my-layer",
            "LayerArn": "arn:aws:lambda:us-east-2:123456789012:layer:my-layer",
            "LatestMatchingVersion": {
                "LayerVersionArn": "arn:aws:lambda:us-east-2:123456789012:layer:my-
layer:2",
                "Version": 2,
                "Description": "My layer",
                "CreatedDate": "2025-04-15T00:37:46.592+0000",
                "CompatibleRuntimes": [
                    "python3.14"
                ]
            }
        }
    ]
}
```

Pour répertorier toutes les couches de votre compte, ignorez l'option `--compatible-runtime`. Les détails de la réponse indiquent la dernière version de chaque couche.

Vous pouvez également obtenir la dernière version d'une couche à l'aide de l'ListLayerVersionsAPI. Par exemple, vous pouvez utiliser la commande CLI `list-layer-versions` suivante :

```
aws lambda list-layer-versions --layer-name my-layer
```

Vous devez voir des résultats similaires à ce qui suit :

```
{
    "LayerVersions": [
        {
            "LayerVersionArn": "arn:aws:lambda:us-east-2:123456789012:layer:my-
layer:2",
            "Version": 2,
            "Description": "My layer",
            "CreatedDate": "2023-11-15T00:37:46.592+0000",
            "CompatibleRuntimes": [
                "java11"
            ]
        },
        {
            "LayerVersionArn": "arn:aws:lambda:us-east-2:123456789012:layer:my-
layer:1",
            "Version": 1,
            "Description": "My layer",
            "CreatedDate": "2023-11-15T00:27:46.592+0000",
            "CompatibleRuntimes": [
                "java11"
            ]
        }
    ]
}
```

Utilisation AWS CloudFormation avec couches

Vous pouvez l'utiliser CloudFormation pour créer une couche et l'associer à votre fonction d'événement Lambda. L'exemple de modèle suivant crée une couche nommée `my-lambda-layer` et l'attache à la fonction d'événement à l'aide de la propriété Layers.

Dans cet exemple, le modèle indique l'Amazon Resource Name (ARN) d'un rôle d'exécution IAM existant. Vous pouvez également créer un nouveau rôle d'exécution dans le modèle à l'aide de la ressource CloudFormation AWS : :IAM : :Role.

Votre fonction événementielle n'a pas besoin d'autorisations spéciales pour utiliser les couches.

```
---
Description: CloudFormation Template for Lambda Event Function with Lambda Layer
Resources:
  MyLambdaLayer:
    Type: AWS::Lambda::LayerVersion
    Properties:
      LayerName: my-lambda-layer
      Description: My Lambda Layer
      Content:
        S3Bucket: amzn-s3-demo-bucket
        S3Key: my-layer.zip
      CompatibleRuntimes:
        - python3.9
        - python3.10
        - python3.11

  MyLambdaFunction:
    Type: AWS::Lambda::Function
    Properties:
      FunctionName: my-lambda-function
      Runtime: python3.9
      Handler: index.handler
      Timeout: 10
      Role: arn:aws:iam::111122223333:role/my_lambda_role
      Layers:
        - !Ref MyLambdaLayer
```

Vous pouvez également l'utiliser AWS Serverless Application Model pour gérer les couches. Pour plus d'informations, consultez the section called “Couches avec AWS SAM”.

Utilisation AWS SAM avec couches

Vous pouvez utiliser le AWS Serverless Application Model (AWS SAM) pour automatiser la création de couches dans votre application. Le type de `AWS::Serverless::LayerVersion` ressource crée une version de couche à laquelle vous pouvez faire référence à partir de votre configuration de fonction d'événement Lambda.

```
AWSTemplateFormatVersion: '2010-09-09'
Transform: 'AWS::Serverless-2016-10-31'
Description: AWS SAM Template for Lambda Event Function with Lambda Layer

Resources:
  MyLambdaLayer:
    Type: AWS::Serverless::LayerVersion
    Properties:
      LayerName: my-lambda-layer
      Description: My Lambda Layer
      ContentUri: s3://amzn-s3-demo-bucket/my-layer.zip
      CompatibleRuntimes:
        - python3.9
        - python3.10
        - python3.11

  MyLambdaFunction:
    Type: AWS::Serverless::Function
    Properties:
      FunctionName: MyLambdaFunction
      Runtime: python3.9
      Handler: app.handler
      CodeUri: s3://amzn-s3-demo-bucket/my-function
      Layers:
        - !Ref MyLambdaLayer
```

Améliorez les fonctions d'événement Lambda à l'aide des extensions Lambda

Vous pouvez utiliser les extensions Lambda pour améliorer vos fonctions d'événement Lambda. Par exemple, utilisez les extensions Lambda pour intégrer les fonctions d'événement à vos outils de surveillance, d'observabilité, de sécurité et de gouvernance préférés. Vous pouvez choisir parmi un

vaste éventail d'outils fournis par des partenaires AWS Lambda, ou créer vos propres extensions Lambda.

Lambda prend en charge les extensions externes et internes. Une extension externe s'exécute en tant que processus indépendant dans l'environnement d'exécution et continue de s'exécuter une fois que l'appel de la fonction d'événement est entièrement traité. Comme les extensions s'exécutent en tant que processus distincts, vous pouvez les écrire dans une langue différente de celle de la fonction d'événement. Tous les Exécutions de la fonction Lambda Event prennent en charge des extensions.

Une extension interne s'exécute dans le cadre du processus de runtime. Votre fonction d'événement accède aux extensions internes à l'aide de scripts wrapper ou de mécanismes en cours de processus tels que. `JAVA_TOOL_OPTIONS` Pour plus d'informations, consultez Modification de l'environnement d'exécution.

Vous pouvez ajouter des extensions à une fonction d'événement à l'aide de la console Lambda, du AWS Command Line Interface (AWS CLI) ou des services et outils d'infrastructure en tant que code (IaC) tels que CloudFormation, AWS Serverless Application Model (AWS SAM) et Terraform.

Vous êtes facturé pour le temps d'exécution que l'extension consomme (par incréments de 1 ms). Aucun coût n'est facturé pour l'installation de vos propres extensions. Pour obtenir des informations sur la tarification des extensions, consultez Tarification AWS Lambda. Pour obtenir des informations sur la tarification des extensions de partenaires, consultez les sites web de ces partenaires. Consultez the section called "Partenaires des extensions" pour obtenir la liste des extensions partenaires officielles.

Rubriques

- Environnement d'exécution
- Impact sur les performances et les ressources
- Permissions
- Configuration des extensions Lambda
- AWS Lambda partenaires d'extensions
- Utilisation de l'API d'extensions Lambda pour créer des extensions
- Accès aux données de télémétrie en temps réel pour les extensions à l'aide de l'API de télémétrie

Environnement d’exécution

Lambda invoque votre fonction d'événement dans un environnement d'exécution, qui fournit un environnement d'exécution sécurisé et isolé. L'environnement d'exécution gère les ressources nécessaires à l'exécution de votre fonction d'événement et fournit un support du cycle de vie pour l'exécution et les extensions de la fonction événementielle.

Le cycle de vie de l’environnement d’exécution comprend les phases suivantes :

- **`Init`** : au cours de cette phase, Lambda crée ou libère un environnement d’exécution avec les ressources configurées, télécharge le code pour la fonction et toutes les couches, initialise les extensions, initialise l’exécution et exécute le code d’initialisation de la fonction (code en dehors du gestionnaire principal). La phase `Init` se produit soit lors de la première invocation, soit avant invocations de fonctions si vous avez activé la simultanéité approvisionnée.

  La phase `Init` est fractionnée en trois sous-phases : `Extension init`, `Runtime init` et `Function init`. Ces sous-phases garantissent que toutes les extensions et l’exécution accomplissent leurs tâches de configuration avant l’exécution du code de la fonction.

  Lorsque SnapStart est activé, la phase `Init` se produit lorsque vous publiez une version de la fonction. Lambda enregistre un instantané de l’état de la mémoire et du disque de l’environnement d’exécution initialisé, fait persister l’instantané chiffré et le met en cache pour un accès à faible latence. Si vous avez un hook d’environnement d’exécution avant le point de contrôle, le code s’exécute alors à la fin de la phase `Init`.
- **`Restore`**(SnapStart uniquement) : Lorsque vous appelez une SnapStartfonction pour la première fois et que celle-ci prend de l'ampleur, Lambda reprend les nouveaux environnements d'exécution à partir de l'instantané persistant au lieu d'initialiser la fonction à partir de zéro. Si vous avez un hook d’exécution après restauration, le code s’exécute à la fin de la phase `Restore`. Vous êtes facturé pour la durée des hooks d’exécution après restauration. L’exécution doit se charger et les hooks d’exécution après restauration doivent se terminer dans le délai imparti (10 secondes). Sinon, vous obtiendrez un SnapStartTimeoutException. Lorsque la phase `Restore` se termine, Lambda invoque le gestionnaire de fonction (Phase d’invocation).
- **`Invoke`** : au cours de cette phase, Lambda invoque le gestionnaire de la fonction. Une fois l’exécution de la fonction terminée, Lambda se prépare à gérer une autre invocation de fonction.
- **`Shutdown`**: cette phase se déclenche si la fonction Lambda ne reçoit aucune invocation pendant un certain temps. Au cours de la phase `Shutdown`, Lambda arrête l’exécution, alerte les extensions pour les laisser s’arrêter proprement, puis supprime l’environnement. Lambda envoie à

chaque extension un événement `Shutdown` indiquant que l'environnement est sur le point d'être arrêté.

Au cours de la phase `Init`, Lambda extrait des couches contenant des extensions dans le répertoire `/opt` dans l'environnement d'exécution. Lambda recherche des extensions dans le répertoire `/opt/extensions/`, interprète chaque fichier comme un fichier d'amorçage exécutable pour le lancement de l'extension, puis démarre toutes les extensions en parallèle.

Impact sur les performances et les ressources

La taille des extensions de votre fonction événementielle est prise en compte dans la limite de taille du package de déploiement. Pour une archive de fichier .zip, la taille totale décompressée de la fonction d'événement et de toutes les extensions ne peut pas dépasser la limite de taille du package de déploiement décompressé de 250 Mo.

Les extensions peuvent avoir un impact sur les performances de votre fonction d'événement car elles partagent les ressources de la fonction d'événement telles que le processeur, la mémoire et le stockage. Par exemple, si une extension effectue des opérations de calcul intensives, la durée d'exécution de votre fonction événementielle peut augmenter.

Chaque extension doit terminer son initialisation avant que Lambda n'appelle la fonction d'événement. Par conséquent, une extension qui consomme un temps d'initialisation important peut augmenter la latence de l'invocation de la fonction d'événement.

Pour mesurer le temps supplémentaire nécessaire à l'extension après l'exécution de la fonction d'événement, vous pouvez utiliser la métrique de la `PostRuntimeExtensionsDuration` fonction. Pour mesurer l'augmentation de la mémoire utilisée, vous pouvez utiliser la métrique `MaxMemoryUsed`. Pour comprendre l'impact d'une extension spécifique, vous pouvez exécuter différentes versions de vos fonctions événementielles côte à côte.

> **Note**
>
> La métrique `MaxMemoryUsed` est l'une des métriques collectées par Lambda Insights et non une métrique native Lambda.

Permissions

Les extensions ont accès aux mêmes ressources que les fonctions événementielles. Les extensions étant exécutées dans le même environnement que la fonction d'événement, les autorisations sont partagées entre la fonction d'événement et l'extension.

Pour une archive de fichier .zip, vous pouvez créer un CloudFormation modèle afin de simplifier la tâche consistant à associer la même configuration d'extension, y compris les autorisations Gestion des identités et des accès AWS (IAM), à plusieurs fonctions d'événement.

Configuration des extensions Lambda

Configuration des extensions (archive de fichiers .zip)

Vous pouvez ajouter une extension à votre fonction d'événement Lambda en tant que couche Lambda. À l'aide de couches, vous pouvez partager des extensions au sein de votre organisation ou avec l'ensemble de la communauté des développeurs Lambda. Vous pouvez ajouter une ou plusieurs extensions à une couche. Vous pouvez enregistrer jusqu'à 10 extensions pour une fonction événementielle.

Vous ajoutez l'extension à votre fonction d'événement en utilisant la même méthode que pour n'importe quelle couche. Pour plus d’informations, consultez the section called “Layers”.

Ajouter une extension à votre fonction événementielle (console)

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez une fonction d'événement.
3. Sélectionnez l'onglet Code s'il n'est pas déjà sélectionné.
4. Sous Layers (Couches), sélectionnez Edit (Modifier).
5. Pour Choose a layer (Choisir une couche), sélectionnez Specify an ARN (Spécifier un nom ARN).
6. Pour Specify an ARN (Spécifier un ARN), entrez l’Amazon Resource Name (ARN) d'une couche d'extension.
7. Choisissez Ajouter.

Utilisation des extensions dans les images de conteneur

Vous pouvez ajouter des extensions à votre image de conteneur. Le paramètre d'image du conteneur ENTRYPOINT spécifie le processus principal de la fonction d'événement. Configurez le paramètre ENTRYPOINT dans le Dockerfile ou en tant que remplacement dans la configuration de la fonction d'événement.

Vous pouvez exécuter plusieurs traitements au sein d'un conteneur. Lambda gère le cycle de vie du traitement principal et tous les traitements supplémentaires. Lambda utilise l'API des extensions pour gérer le cycle de vie des extensions.

Exemple : ajout d'une extension externe

Une extension externe s'exécute dans le cadre d'un processus distinct de celui de la fonction d'événement Lambda. Lambda démarre un traitement pour chaque extension dans le répertoire `/opt/extensions/`. Lambda utilise l'API d'extensions pour gérer le cycle de vie des extensions. Une fois que la fonction d'événement est terminée, Lambda envoie un `Shutdown` événement à chaque extension externe.

Example d'ajouter une extension externe à une image de base Python

```
FROM public.ecr.aws/lambda/python:3.11

# Copy and install the app
COPY /app /app
WORKDIR /app
RUN pip install -r requirements.txt

# Add an extension from the local directory into /opt/extensions
ADD my-extension.zip /opt/extensions
CMD python ./my-function.py
```

Étapes suivantes

Pour de plus amples informations sur les extensions, nous vous recommandons les ressources suivantes :

- Pour un exemple pratique de base, consultez la section Création d'extensions pour AWS Lambda sur le blog AWS Compute.
- Pour plus d'informations sur les extensions proposées par AWS Lambda les partenaires, consultez la section Présentation des AWS Lambda extensions sur le blog AWS Compute.
- Pour consulter les exemples d'extensions et de scripts wrapper disponibles, consultez la section AWS Lambda Extensions du GitHub référentiel AWS Samples.

AWS Lambda partenaires d'extensions

AWS Lambda s'est associé à plusieurs entités tierces pour fournir des extensions à intégrer à vos fonctions d'événement Lambda. La liste suivante détaille les extensions tierces qui sont prêtes à être utilisées à tout moment.

- AppDynamics— Fournit une instrumentation automatique des fonctions Node.js d'événement Lambda en Python, fournissant de la visibilité et des alertes sur les performances des fonctions d'événement.
- Axiom— Fournit des tableaux de bord pour surveiller les performances de la fonction d'événement Lambda et les mesures agrégées au niveau du système.
- Datadog : offre une visibilité complète en temps réel pour vos applications sans serveur grâce à l'utilisation de métriques, de traces et de journaux.
- Dynatrace— Fournit une visibilité sur les traces et les métriques, et utilise l'IA pour la détection automatique des erreurs et l'analyse des causes premières sur l'ensemble du stack applicatif.
- Elastic : offre une surveillance de la performance des applications (APM) pour identifier et résoudre la cause profonde des problèmes à l'aide de traces, de métriques et de journaux corrélés.
- Epsagon— Écoute les événements d'invocation, stocke les traces et les envoie en parallèle aux exécutions de la fonction d'événement Lambda.
- Fastly— Protège vos fonctions d'événement Lambda contre les activités suspectes, telles que les attaques par injection, le piratage de compte par le biais du bourrage d'informations d'identification, les robots malveillants et l'utilisation abusive des API.
- HashiCorp Vault— Gère les secrets et les met à la disposition des développeurs pour qu'ils puissent les utiliser dans le code Event Function, sans qu'Event Functions Vault ne soit au courant.
- Honeycomb : outil d'observabilité pour déboguer votre pile d'applications.
- Lumigo— Profile les invocations de la fonction d'événement Lambda et collecte des métriques pour résoudre les problèmes dans les environnements sans serveur et de microservices.
- New Relic— Fonctionne parallèlement aux fonctions d'événements Lambda, qui collectent, améliorent et transportent automatiquement la télémétrie vers la plateforme d'observabilité unifiée de New Relic.
- Sedai— Une plateforme de gestion du cloud autonome, alimentée par AI/ML, qui fournit une optimisation continue aux équipes chargées des opérations cloud afin de maximiser les économies, les performances et la disponibilité du cloud à grande échelle.
- Sentry— Diagnostiquez, corrigez et optimisez les performances des fonctions d'événement Lambda.

- Site24x7 : permet une observabilité en temps réel dans vos environnements Lambda.
- Splunk— Collecte des métriques à haute résolution et à faible latence pour une surveillance efficace des fonctions d'événements Lambda.
- Sumo Logic : offre une visibilité sur l'état et les performances des applications sans serveur.
- Salt Security — Simplifie la gouvernance de la posture des API et la sécurité des API pour Lambda Event Functions grâce à une configuration automatisée et à une prise en charge de divers environnements d'exécution.

AWS extensions gérées

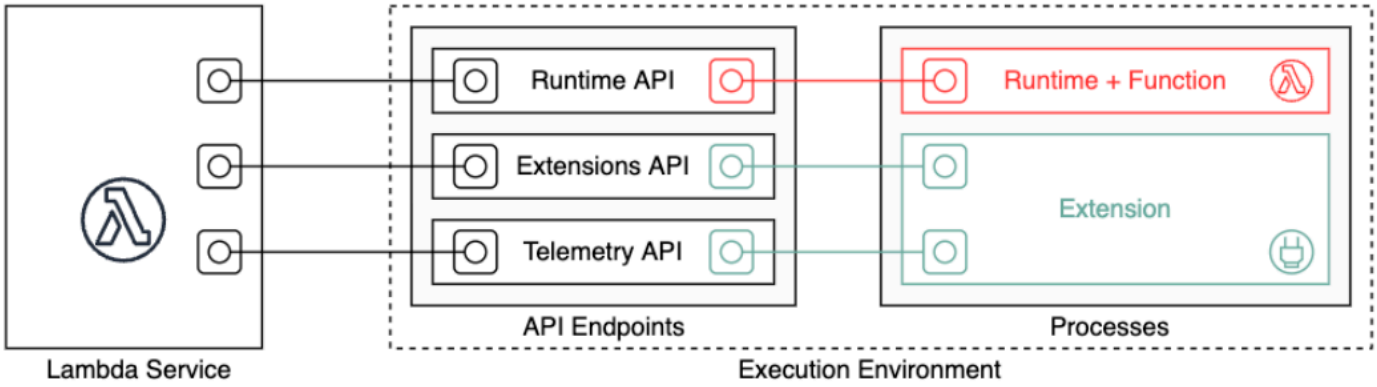
AWS fournit ses propres extensions gérées, notamment :

- AWS AppConfig— Utilisez des indicateurs de fonctionnalité et des données dynamiques pour mettre à jour vos fonctions d'événement Lambda. Vous pouvez également utiliser cette extension pour mettre à jour d'autres configurations dynamiques, telles que la limitation et le réglage des opérations.
- Amazon CodeGuru Profiler — Améliore les performances des applications et réduit les coûts en identifiant la ligne de code la plus coûteuse d'une application et en fournissant des recommandations pour améliorer le code.
- CloudWatch Lambda Insights — Surveillez, dépannez et optimisez les performances de vos fonctions d'événements Lambda grâce à des tableaux de bord automatisés.
- AWS Distro for OpenTelemetry (ADOT) — Permet à Event Functions d'envoyer des données de AWS suivi à des services de surveillance tels que AWS X-Ray, et à des destinations compatibles, OpenTelemetry tels que Honeycomb et Lightstep.
- AWS Paramètres et secrets : récupérez en toute sécurité les paramètres depuis le magasin de AWS Systems Manager paramètres et les secrets depuis AWS Secrets Manager Lambda Event Functions.

Pour plus d'exemples d'extensions supplémentaires et de projets de démonstration, voir Extensions AWS Lambda.

Utilisation de l'API d'extensions Lambda pour créer des extensions

Les auteurs de fonctions d'événement Lambda utilisent des extensions pour intégrer Lambda à leurs outils préférés de surveillance, d'observabilité, de sécurité et de gouvernance. Les auteurs de fonctions événementielles peuvent utiliser des extensions issues de AWS projets open source, de AWS partenaires et de projets open source. Pour plus d'informations sur l'utilisation des extensions, consultez la section Présentation des AWS Lambda extensions sur le blog AWS Compute. Cette section décrit comment utiliser l'API Extensions Lambda, le cycle de vie de l'environnement d'exécution Lambda et la référence de l'API Extensions Lambda.



En tant qu'auteur d'extension, vous pouvez utiliser l'API d'extensions Lambda pour opérer une intégration profonde à l'environnement d'exécution Lambda. Votre extension peut s'enregistrer pour les événements relatifs à la fonction d'événement et au cycle de vie de l'environnement d'exécution. En réponse à ces événements, vous pouvez démarrer de nouveaux processus, exécuter une logique, ainsi que contrôler et orienter toutes les phases du cycle de vie Lambda : initialisation, appel et arrêt. En outre, vous pouvez utiliser l'API Runtime Logs pour recevoir un flux de journaux.

Une extension s'exécute en tant que processus indépendant dans l'environnement d'exécution et peut continuer à s'exécuter une fois que l'appel de la fonction d'événement est entièrement traité. Comme les extensions s'exécutent en tant que processus, vous pouvez les écrire dans un langage différent de celui de la fonction d'événement. Nous vous recommandons d'implémenter des extensions à l'aide d'un langage compilé.

Dans ce cas, l'extension est un fichier binaire autonome compatible avec les environnements d'exécution pris en charge. Tous les Exécutions de la fonction Lambda Event prennent en charge des extensions. Si vous utilisez un langage non compilé, assurez-vous d'inclure un environnement d'exécution compatible dans l'extension.

Lambda prend également en charge les extensions internes. Une extension interne s'exécute comme un thread séparé dans le processus d'exécution. L'exécution démarre et arrête l'extension interne. Un autre mode d'intégration à l'environnement Lambda consiste à utiliser des variables d'environnement spécifiques au langage et des scripts encapsuleurs. Vous pouvez utiliser ces paramètres pour configurer l'environnement d'exécution et modifier le comportement de démarrage du processus d'exécution.

Vous pouvez ajouter des extensions à une fonction d'événement de deux manières. Pour une fonction d'événement déployée sous forme d'archive de fichier .zip, vous déployez votre extension sous forme de couche. Pour une fonction d'événement définie comme une image de conteneur, vous ajoutez les extensions à votre image de conteneur.

> **Note**
>
> Pour des exemples d'extensions et de scripts wrapper, voir AWS Lambda Extensions dans le GitHub référentiel AWS Samples.

Rubriques

- Cycle de vie d'un environnement d'exécution Lambda
- Référence d'API d'extensions

Cycle de vie d'un environnement d'exécution Lambda

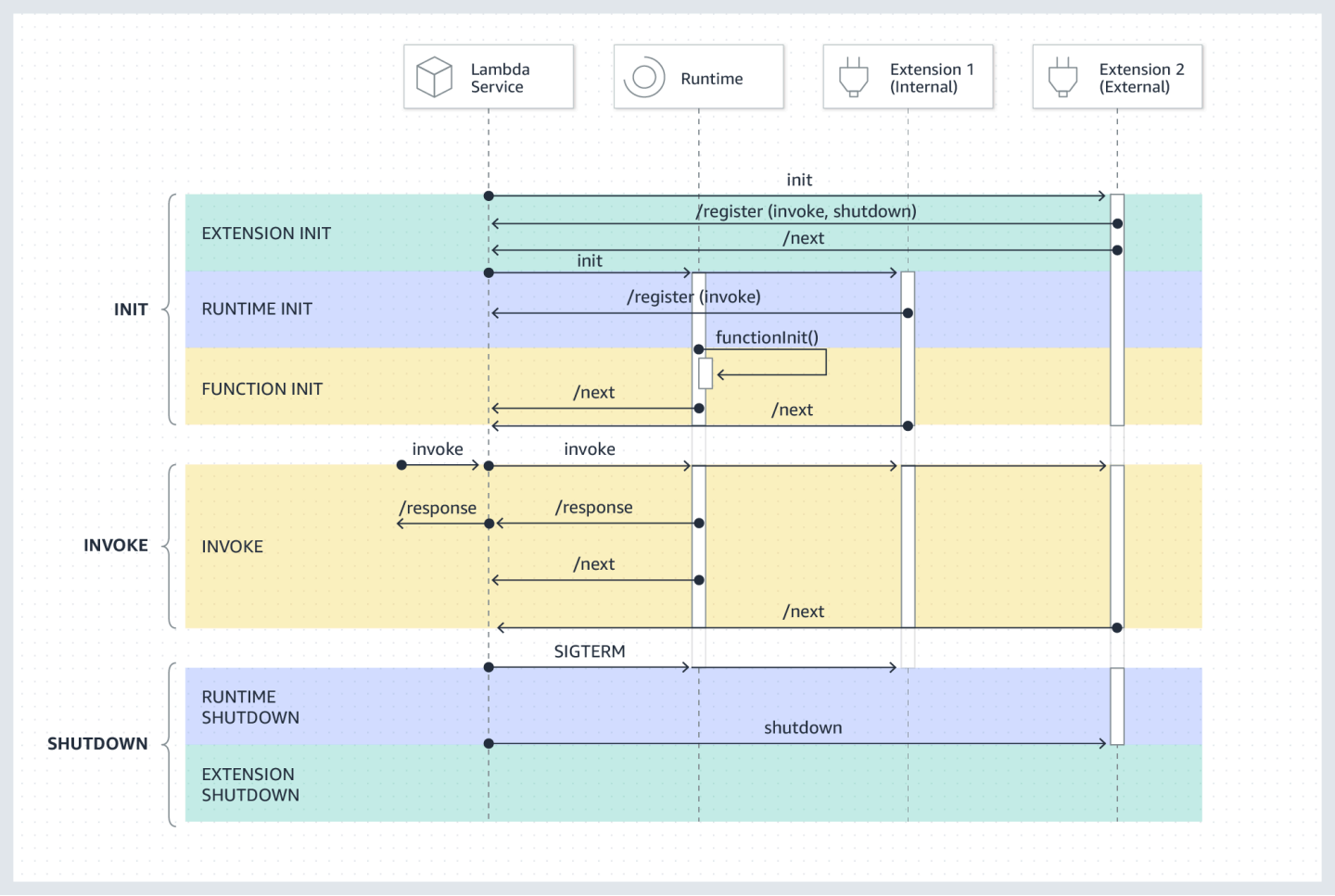
Le cycle de vie de l'environnement d'exécution comprend les phases suivantes :

- **`Init`**: Dans cette phase, Lambda crée ou débloque un environnement d'exécution avec les ressources configurées, télécharge le code de la fonction d'événement et de toutes les couches, initialise les extensions, initialise le runtime, puis exécute le code d'initialisation de la fonction d'événement (le code extérieur au gestionnaire principal). La `Init` phase a lieu soit lors de la première invocation, soit avant les invocations de la fonction d'événement si vous avez activé la simultanéité provisionnée.

  La phase `Init` est fractionnée en trois sous-phases : `Extension init`, `Runtime init` et `Function init`. Ces sous-phases garantissent que toutes les extensions et le moteur d'exécution terminent leurs tâches de configuration avant l'exécution du code Event Function.

- **`Invoke`**: Dans cette phase, Lambda appelle le gestionnaire Event Function. Une fois que la fonction d'événement est terminée, Lambda se prépare à gérer un autre appel de fonction d'événement.
- **`Shutdown`**: Cette phase est déclenchée si la fonction d'événement Lambda ne reçoit aucune invocation pendant un certain temps. Au cours de la phase `Shutdown`, Lambda arrête l'exécution, alerte les extensions pour les laisser s'arrêter proprement, puis supprime l'environnement. Lambda envoie à chaque extension un événement `Shutdown` indiquant que l'environnement est sur le point d'être arrêté.

Chaque phase commence par un événement que Lambda envoie au runtime et à toutes les extensions enregistrées. L'exécution et chaque extension signalent la fin de l'opération en envoyant une requête d'API `Next`. Lambda bloque l'environnement d'exécution lorsque l'exécution de chaque processus est terminée, et qu'il n'y a pas d'événement en attente.



Rubriques

- Phase d’initialisation
- Phase d’invocation
- Phase d’arrêt
- Autorisations et configuration
- Gestion des défaillances
- Dépannage des extensions

Phase d’initialisation

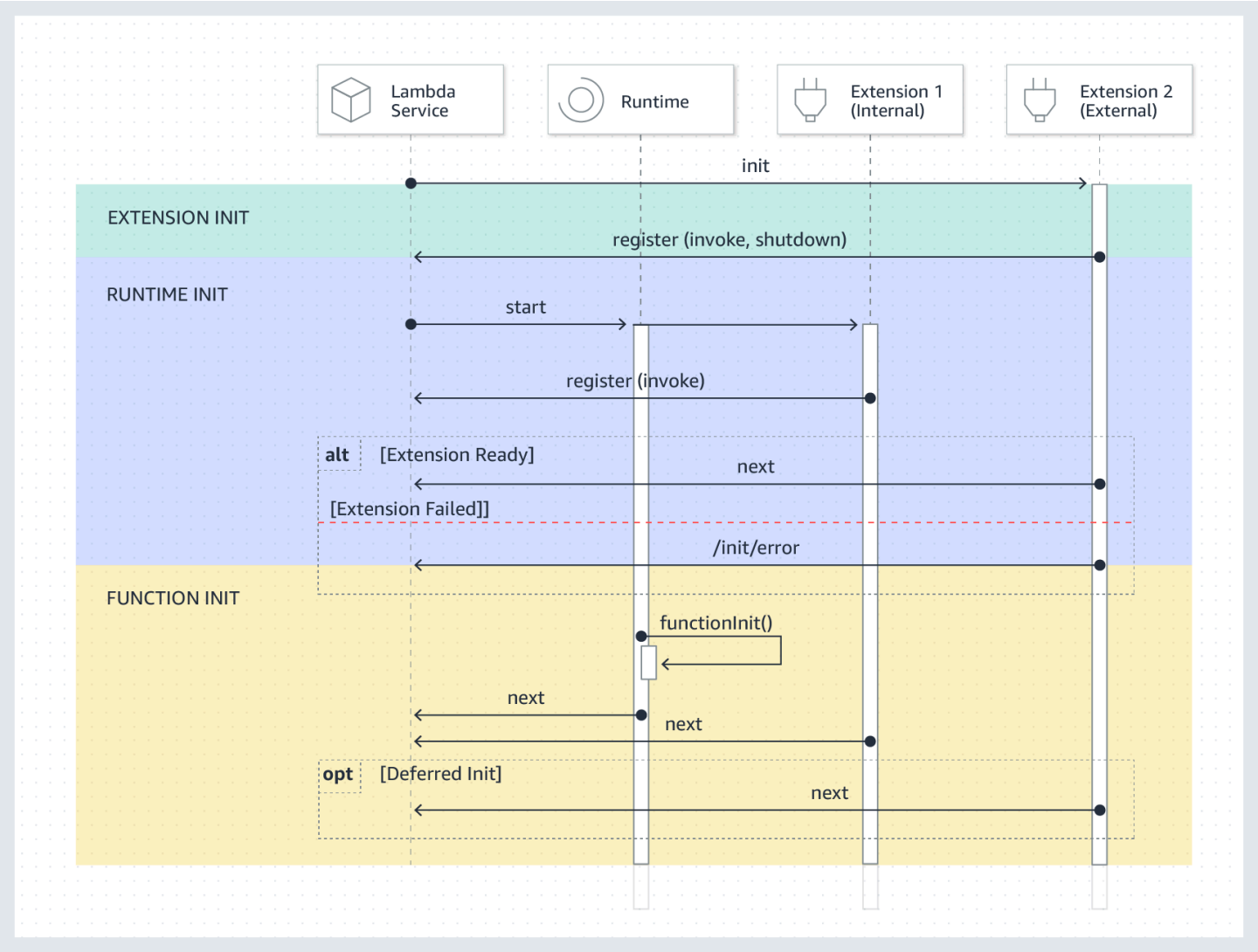
Au cours de la phase `Extension init`, chaque extension doit s’enregistrer auprès de Lambda pour recevoir des événements. Lambda utilise le nom de fichier complet de l’extension pour vérifier que la séquence d’amorçage de celle-ci est terminée. Par conséquent, chaque appel d’API `Register` doit inclure l’en-tête `Lambda-Extension-Name` avec le nom de fichier complet de l’extension.

Vous pouvez enregistrer jusqu'à 10 extensions pour une fonction événementielle. Cette limite est appliquée via l’appel d’API `Register`.

Après l’enregistrement de chaque extension, Lambda démarre la phase `Runtime init`. Le processus d’exécution appelle `functionInit` pour démarrer la phase `Function init`.

La phase `Init` se termine lorsque l’environnement d’exécution et chaque extension enregistrée indiquent la fin de l’opération en envoyant une demande d’API `Next`.

> **Note**
>
> Les extensions peuvent terminer leur initialisation à n’importe quel moment de la phase `Init`.



Phase d'invocation

Lorsqu'une fonction d'événement Lambda est invoquée en réponse à une demande d'`Next`API, Lambda envoie un `Invoke` événement au moteur d'exécution et à chaque extension enregistrée pour l'événement. `Invoke`

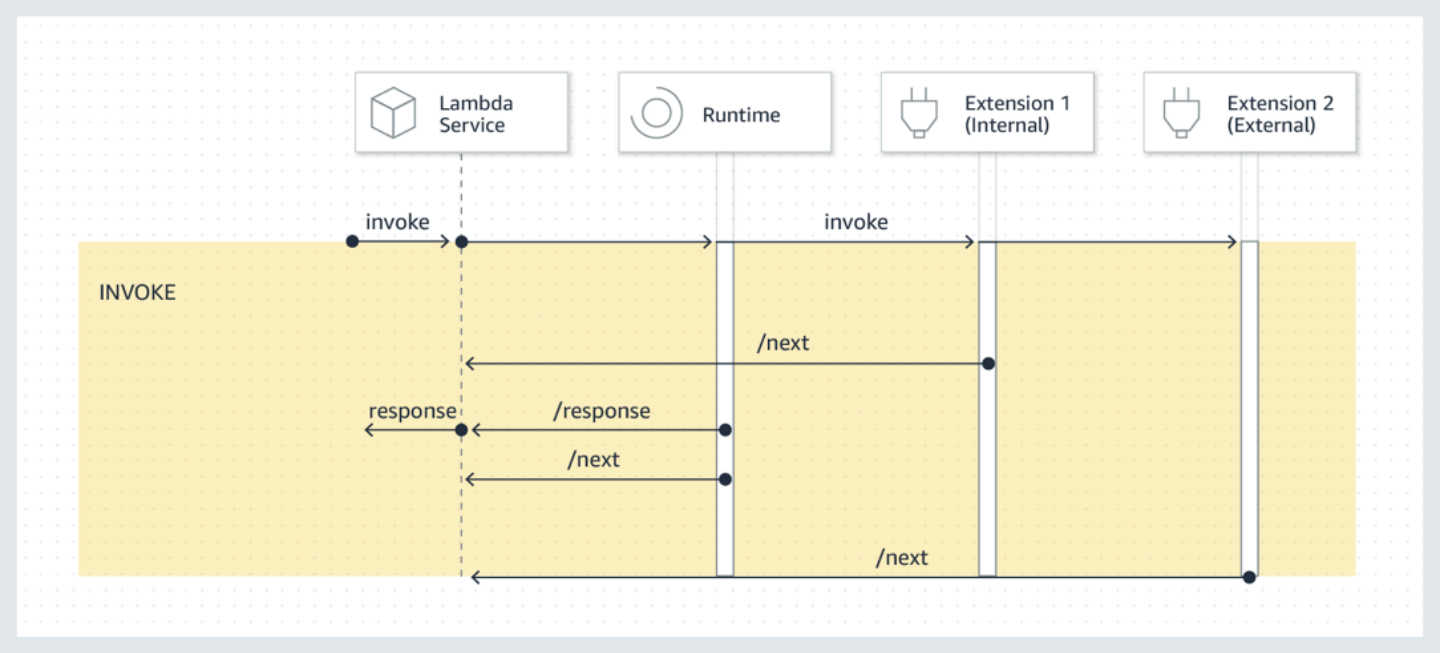
> **Note**
>
> Instances gérées Lambda : les extensions pour les fonctions des instances gérées Lambda ne peuvent pas être enregistrées pour l'événement. `Invoke` Comme les instances gérées Lambda prennent en charge les appels simultanés au sein d'un même environnement d'exécution, l'`Invoke`événement n'est pas pris en charge. Les extensions ne peuvent être

enregistrées que pour l'`Shutdown`événement. Si vous devez suivre le début et la fin des invocations, utilisez l'événement de `platform.report` plateforme via l'API de télémétrie.

Pendant l'invocation, les extensions externes s'exécutent en parallèle avec la fonction d'événement. Ils continuent également de fonctionner une fois la fonction d'événement terminée. Vous pouvez l'utiliser pour capturer des informations de diagnostic ou pour envoyer des journaux, des métriques et des traces à l'emplacement de votre choix.

Après avoir reçu la réponse de la fonction d'événement du moteur d'exécution, Lambda renvoie la réponse au client, même si les extensions sont toujours en cours d'exécution.

La phase `Invoke` prend fin lorsque l'environnement d'exécution et toutes les extensions signalent qu'ils ont terminé en envoyant une demande d'API `Next`.



Charge utile de l'événement : l'événement envoyé au moteur d'exécution (et à la fonction d'événement Lambda) contient l'intégralité de la demande, des en-têtes (`RequestId`tels que) et de la charge utile. L'événement envoyé à chaque extension contient des métadonnées décrivant le contenu de l'événement. Cet événement du cycle de vie inclut le type d'événement, l'heure à laquelle la fonction d'événement expire (`deadlineMs`)`requestId`, le nom de ressource Amazon (ARN) de la fonction d'événement invoquée et les en-têtes de suivi.

Les extensions qui souhaitent accéder au corps de l'événement Event Function peuvent utiliser un SDK en cours d'exécution qui communique avec l'extension. Les développeurs de fonctions

d'événement utilisent le SDK intégré à l'exécution pour envoyer la charge utile à l'extension lorsque la fonction d'événement est invoquée.

Voici un exemple de charge utile :

```
{
    "eventType": "INVOKE",
    "deadlineMs": 676051,
    "requestId": "3da1f2dc-3222-475e-9205-e2e6c6318895",
    "invokedFunctionArn": "arn:aws:lambda:us-
east-1:123456789012:function:ExtensionTest",
    "tracing": {
        "type": "X-Amzn-Trace-Id",
        "value":
 "Root=1-5f35ae12-0c0fec141ab77a00bc047aa2;Parent=2be948a625588e32;Sampled=1"
    }
 }
```

Limite de durée : le paramètre de temporisation de la fonction d'événement limite la durée de l'ensemble de la `Invoke` phase. Par exemple, si vous définissez le délai d'expiration de la fonction d'événement à 360 secondes, la fonction d'événement et toutes les extensions doivent être terminées dans les 360 secondes. Notez qu'il n'y a pas de phase post-invocation indépendante. La durée est le temps total nécessaire à votre exécution et à toutes les invocations de vos extensions pour terminer. Elle n'est calculée qu'une fois que la fonction événement et toutes les extensions ont fini de s'exécuter.

Impact sur les performances et surcharge des extensions : les extensions peuvent avoir un impact sur les performances de la fonction événementielle. En tant qu'auteur d'extension, vous contrôlez l'impact de votre extension sur les performances. Par exemple, si votre extension effectue des opérations de calcul intensives, la durée de la fonction d'événement augmente car l'extension et le code de la fonction d'événement partagent les mêmes ressources du processeur. En outre, si votre extension effectue des opérations étendues une fois l'invocation de la fonction d'événement terminée, la durée de la fonction d'événement augmente car la `Invoke` phase se poursuit jusqu'à ce que toutes les extensions signalent qu'elles sont terminées.

> **Note**
>
> Lambda alloue la puissance du processeur proportionnellement aux paramètres de mémoire de la fonction d'événement. La durée d'exécution et d'initialisation peut augmenter lorsque les paramètres de mémoire sont faibles, car la fonction d'événement et les processus d'extension

se disputent les mêmes ressources du processeur. Pour réduire la durée d'exécution et d'initialisation, essayez d'augmenter le paramètre de mémoire.

Pour vous aider à déterminer l'impact sur les performances des extensions dans la phase `Invoke`, Lambda génère la métrique `PostRuntimeExtensionsDuration`. Cette métrique mesure le temps cumulé qui s'écoule entre la demande d'API `Next` de l'environnement d'exécution et la dernière demande d'API `Next` d'une extension. La métrique `MaxMemoryUsed` permet de mesurer l'augmentation de la mémoire utilisée. Pour plus d'informations sur les métriques des fonctions événementielles, consultezUtilisation de CloudWatch métriques avec Lambda.

Les développeurs de fonctions d'événement peuvent exécuter différentes versions de leurs fonctions d'événement côte à côte pour comprendre l'impact d'une extension spécifique. Nous recommandons aux auteurs d'extensions de publier la consommation de ressources prévue afin de permettre aux développeurs de fonctions événementielles de choisir plus facilement une extension adaptée.

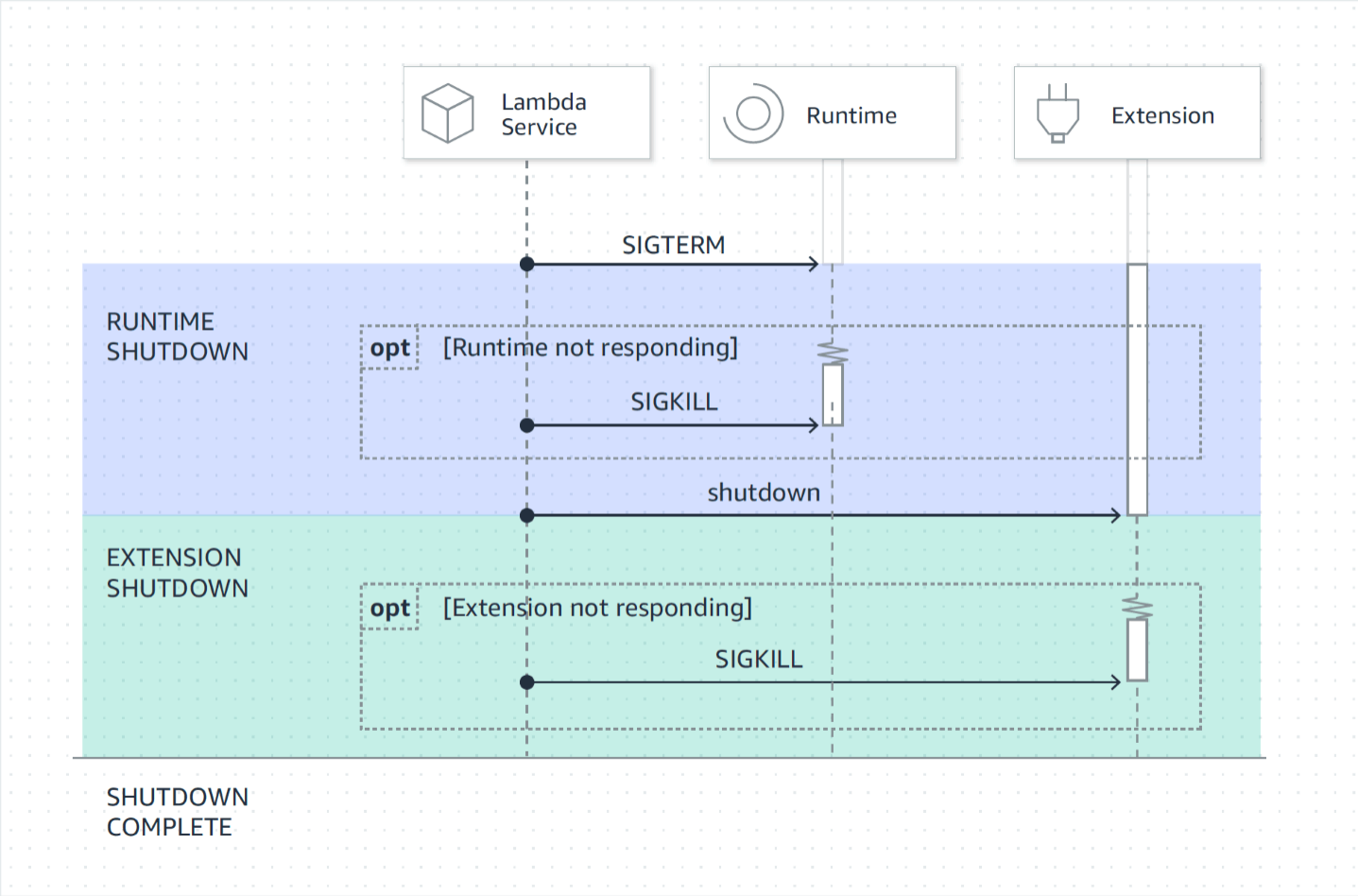
Phase d'arrêt

Quand Lambda est sur le point d'arrêter l'exécution, il envoie un `Shutdown` à chaque extension externe enregistrée. Les extensions peuvent utiliser ce temps pour les tâches de nettoyage final. L'événement `Shutdown` est envoyé en réponse à une demande d'API `Next`.

Limite de durée : la durée maximale de la phase `Shutdown` dépend de la configuration des extensions enregistrées :

- 0 ms : fonction sans extension enregistrée
- 500 ms : fonction avec une extension interne enregistrée.
- 2 000 ms : fonction avec une ou plusieurs extensions externes enregistrées.

Si l'environnement d'exécution ou une extension ne répondent pas à l'événement `Shutdown` dans cette limite de temps, Lambda met fin au processus à l'aide d'un signal `SIGKILL`.



Charge utile d'événement : l'événement `Shutdown` contient la raison de l'arrêt et le temps restant en millisecondes.

`shutdownReason` contient les éléments suivants :

- SPINDOWN – Arrêt normal
- TIMEOUT – Limite de durée dépassée
- ÉCHEC : condition d'erreur, telle qu'un événement `out-of-memory`

```
{
  "eventType": "SHUTDOWN",
  "shutdownReason": "reason for shutdown",
  "deadlineMs": "the time and date that the function times out in Unix time
 milliseconds"
}
```

Autorisations et configuration

Les extensions s'exécutent dans le même environnement d'exécution que la fonction d'événement Lambda. Les extensions partagent également des ressources avec la fonction d'événement, telles que le processeur, la mémoire et `/tmp` le stockage sur disque. En outre, les extensions utilisent le même rôle Gestion des identités et des accès AWS (IAM) et le même contexte de sécurité que la fonction d'événement.

Autorisations d'accès au système de fichiers et au réseau : les extensions s'exécutent dans le même espace de noms de système de fichiers et de réseau que le moteur d'exécution d'Event Function. Cela signifie que les extensions doivent être compatibles avec le système d'exploitation associé. Si une extension nécessite des règles de trafic réseau sortant supplémentaires, vous devez appliquer ces règles à la configuration de la fonction d'événement.

> **Note**
>
> Le répertoire du code de la fonction d'événement étant en lecture seule, les extensions ne peuvent pas modifier le code de la fonction d'événement.

Variables d'environnement : les extensions peuvent accéder aux variables d'environnement de la fonction d'événement, à l'exception des variables suivantes qui sont spécifiques au processus d'exécution :

- `AWS_EXECUTION_ENV`
- `AWS_LAMBDA_LOG_GROUP_NAME`
- `AWS_LAMBDA_LOG_STREAM_NAME`
- `AWS_XRAY_CONTEXT_MISSING`
- `AWS_XRAY_DAEMON_ADDRESS`
- `LAMBDA_RUNTIME_DIR`
- `LAMBDA_TASK_ROOT`
- `_AWS_XRAY_DAEMON_ADDRESS`
- `_AWS_XRAY_DAEMON_PORT`
- `_HANDLER`

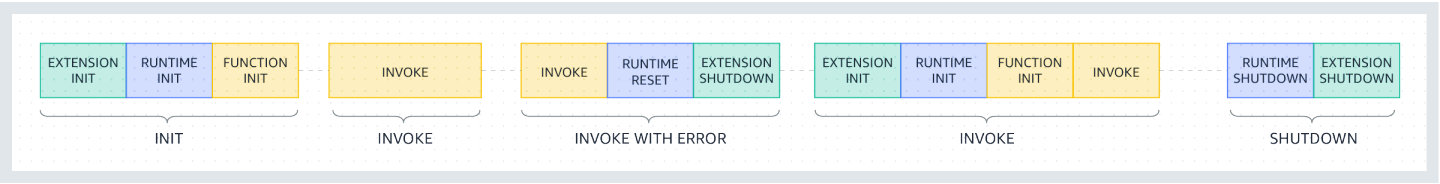
> **Note**
>
> Détection des instances gérées Lambda : les extensions peuvent vérifier la variable d'`AWS_LAMBDA_INITIALIZATION_TYPE`environnement pour déterminer si elles s'exécutent sur des instances gérées Lambda plutôt que sur des fonctions Lambda (par défaut). Il s'agit de la méthode recommandée pour que les extensions adaptent leur comportement en fonction du type d'environnement d'exécution.

Gestion des défaillances

Échecs d'initialisation : si une extension échoue, Lambda redémarre l'environnement d'exécution pour assurer un comportement cohérent et encourager un échec rapide des extensions. En outre, pour certains clients, les extensions doivent répondre à des besoins stratégiques tels que la journalisation, la sécurité, la gouvernance et la collecte de télémétrie.

Défaillances d'appel (telles que le manque de mémoire ou le délai d'expiration de la fonction d'événement) : étant donné que les extensions partagent des ressources avec le moteur d'exécution, l'épuisement de la mémoire les affecte. Lorsque l'environnement d'exécution échoue, toutes les extensions et l'environnement d'exécution lui-même participent à la phase `Shutdown`. En outre, le moteur d'exécution est redémarré, soit automatiquement dans le cadre de l'appel en cours, soit par le biais d'un mécanisme de réinitialisation différée.

En cas de défaillance (expiration d'une fonction d'événement ou erreur d'exécution, par exemple)`Invoke`, le service Lambda effectue une réinitialisation. La réinitialisation se comporte comme un événement `Shutdown`. Lambda commence par arrêter l'environnement d'exécution, puis envoie un événement `Shutdown` à chaque extension externe enregistrée. L'événement comprend le motif de l'arrêt. Si cet environnement est utilisé pour un nouvel appel, l'extension et l'environnement d'exécution sont réinitialisés dans le cadre de l'appel suivant.



Pour une explication plus détaillée du diagramme précédent, consultez Échecs pendant la phase d'invocation.

Journaux des extensions : Lambda envoie le résultat du journal des extensions à CloudWatch Logs. Lambda génère également un événement de journal supplémentaire pour chaque extension

pendant la phase `Init`. L'événement de journal enregistre le nom et la préférence d'enregistrement (événement, configuration) en cas de succès, ou la raison de l'échec le cas échéant.

Dépannage des extensions

- Si une demande `Register` échoue, assurez-vous que l'en-tête `Lambda-Extension-Name` de l'appel d'API `Register` contient le nom de fichier complet de l'extension.
- Si la demande `Register` échoue pour une extension interne, assurez-vous que la demande n'est pas enregistrée pour l'événement `Shutdown`.

Référence d'API d'extensions

La spécification OpenAPI pour l'API d'extensions version 2020-01-01 est disponible ici : extensions-api.zip

Vous pouvez extraire la valeur du point de terminaison d'API à partir de la variable d'environnement `AWS_LAMBDA_RUNTIME_API`. Pour envoyer une demande `Register`, utilisez le préfixe `2020-01-01/` avant chaque chemin d'API. Exemples :

```
http://${AWS_LAMBDA_RUNTIME_API}/2020-01-01/extension/register
```

Méthodes d'API

- Enregistrement
- Suivant
- Erreur d'initiation
- Erreur de sortie

Enregistrement

Au cours de la phase `Extension init`, chaque extension doit s'enregistrer auprès de Lambda pour recevoir les événements. Lambda utilise le nom de fichier complet de l'extension pour vérifier que la séquence d'amorçage de celle-ci est terminée. Par conséquent, chaque appel d'API `Register` doit inclure l'en-tête `Lambda-Extension-Name` avec le nom de fichier complet de l'extension.

Les extensions internes sont lancées et arrêtées par le processus d'environnement d'exécution, de sorte qu'elles ne peuvent pas être enregistrées pour l'événement `Shutdown`.

Chemin – `/extension/register`

Méthode – POST

En-têtes de demandes

- `Lambda-Extension-Name` : nom de fichier complet de l'extension. Obligatoire : oui. Type : string.
- `Lambda-Extension-Accept-Feature` – Utilisez ceci pour spécifier les fonctionnalités optionnelles d'Extensions pendant l'enregistrement. Requis : non. Type : chaîne séparée par des virgules. Fonctions disponibles pour spécifier en utilisant ce paramètre :
  - `accountId`— Si elle est spécifiée, la réponse d'enregistrement de l'extension contient l'ID de compte associé à la fonction d'événement Lambda pour laquelle vous enregistrez l'extension.

Paramètres du corps de la demande

- `events` : tableau des événements pour lesquels s'enregistrer. Requis : non. Type : tableau de chaînes. Chaînes valides : `INVOKE`, `SHUTDOWN`.

> **Note**
>
> Instances gérées Lambda : les extensions pour les fonctions des instances gérées Lambda ne peuvent être enregistrées que pour l'événement. `SHUTDOWN` Toute tentative d'inscription à l'`INVOKE`événement entraîne une erreur. Cela est dû au fait que les instances gérées Lambda prennent en charge les appels simultanés au sein d'un environnement d'exécution unique.

En-têtes de réponse

- `Lambda-Extension-Identifier` : identifiant d'agent unique généré (chaîne UUID) requis pour toutes les requêtes subséquentes.

Codes de réponse

- 200 – Corps de la réponse contenant le nom de la fonction, la version de la fonction et le nom du gestionnaire.
- 400 – Demande erronée.
- 403 – Interdit

- 500 — Erreur du conteneur. Non-recoverable état. L'extension doit se fermer rapidement.

Example Exemple de corps de la demande

```
{
    'events': [ 'INVOKE', 'SHUTDOWN']
}
```

Example Exemple de corps de la réponse

```
{
    "functionName": "helloWorld",
    "functionVersion": "$LATEST",
    "handler": "lambda_function.lambda_handler"
}
```

Example Exemple de corps de réponse avec la fonction optionnelle accountId

```
{
    "functionName": "helloWorld",
    "functionVersion": "$LATEST",
    "handler": "lambda_function.lambda_handler",
    "accountId": "123456789012"
}
```

Suivant

Les extensions envoient une demande d'API `Next` pour recevoir l'événement suivant, qui peut être un événement `Invoke` ou un événement `Shutdown`. Le corps de la réponse contient la charge utile, sous la forme d'un document JSON contenant des données d'événement.

L'extension envoie une demande d'API `Next` pour signaler qu'elle est prête à recevoir de nouveaux événements. Il s'agit d'un appel bloquant.

Ne définissez pas de délai d'expiration sur l'appel GET, car l'extension peut être suspendue pendant un certain temps jusqu'à ce qu'il y ait un événement à retourner.

Chemin – `/extension/event/next`

Méthode – GET

En-têtes de demandes

- `Lambda-Extension-Identifier` : identifiant unique pour l'extension (chaîne UUID). Obligatoire : oui. Type : chaîne UUID.

En-têtes de réponse

- `Lambda-Extension-Event-Identifier` : identifiant unique pour l'événement (chaîne UUID).

Codes de réponse

- 200 : réponse contenant des informations sur l'événement suivant (`EventInvoke` ou `EventShutdown`).
- 403 – Interdit.
- 500 — Erreur du conteneur. Non-recoverable état. L'extension doit se fermer rapidement.

Erreur d'initiation

L'extension utilise cette méthode pour signaler une erreur d'initialisation à Lambda. Appelez-la lorsque l'extension ne parvient pas à s'initialiser après son enregistrement. Après que Lambda a reçu l'erreur, aucun autre appel d'API n'aboutit. L'extension doit quitter après avoir reçu la réponse de Lambda.

Chemin – `/extension/init/error`

Méthode – POST

En-têtes de demandes

- `Lambda-Extension-Identifier` : identifiant unique pour l'extension. Obligatoire : oui. Type : chaîne UUID.
- `Lambda-Extension-Function-Error-Type` – Type d'erreur rencontré par l'extension. Obligatoire : oui. Cet en-tête se compose d'une valeur de chaîne. Lambda accepte n'importe quelle chaîne, mais nous recommandons le format <category.reason>. Par exemple :
  - Extension.NoSuchHandler
  - Extension.APIKeyNotFound
  - Extension.ConfigInvalid

- Extension.UnknownReason

Paramètres du corps de la demande

- `ErrorRequest` : informations sur l'erreur. Requis : non.

Ce champ est un objet JSON avec la structure suivante :

```
{
      errorMessage: string (text description of the error),
      errorType: string,
      stackTrace: array of strings
}
```

Notez que Lambda accepte n'importe quelle valeur pour `errorType`.

L'exemple suivant montre un message d'erreur de fonction Lambda indiquant que la fonction n'a pas pu analyser les données d'événement fournies dans l'invocation.

Example Erreur de fonction

```
{
      "errorMessage" : "Error parsing event data.",
      "errorType" : "InvalidEventDataException",
      "stackTrace": [ ]
}
```

Codes de réponse

- 202 – Accepté
- 400 – Demande erronée.
- 403 – Interdit
- 500 — Erreur du conteneur. Non-recoverable état. L'extension doit se fermer rapidement.

Erreur de sortie

L'extension utilise cette méthode pour signaler une erreur à Lambda avant de quitter. Appelez-la lorsque vous rencontrez une défaillance inattendue. Après que Lambda a reçu l'erreur, aucun autre appel d'API n'aboutit. L'extension doit quitter après avoir reçu la réponse de Lambda.

Chemin – `/extension/exit/error`

Méthode – POST

En-têtes de demandes

- `Lambda-Extension-Identifier` : identifiant unique pour l'extension. Obligatoire : oui. Type : chaîne UUID.
- `Lambda-Extension-Function-Error-Type` – Type d'erreur rencontré par l'extension. Obligatoire : oui. Cet en-tête se compose d'une valeur de chaîne. Lambda accepte n'importe quelle chaîne, mais nous recommandons le format <category.reason>. Par exemple :
  - Extension.NoSuchHandler
  - Extension.APIKeyNotFound
  - Extension.ConfigInvalid
  - Extension.UnknownReason

Paramètres du corps de la demande

- `ErrorRequest` : informations sur l'erreur. Requis : non.

Ce champ est un objet JSON avec la structure suivante :

```
{
      errorMessage: string (text description of the error),
      errorType: string,
      stackTrace: array of strings
}
```

Notez que Lambda accepte n'importe quelle valeur pour `errorType`.

L'exemple suivant montre un message d'erreur de fonction Lambda indiquant que la fonction n'a pas pu analyser les données d'événement fournies dans l'invocation.

Example Erreur de fonction

```
{
      "errorMessage" : "Error parsing event data.",
      "errorType" : "InvalidEventDataException",
```

```
      "stackTrace": [ ]
}
```

Codes de réponse

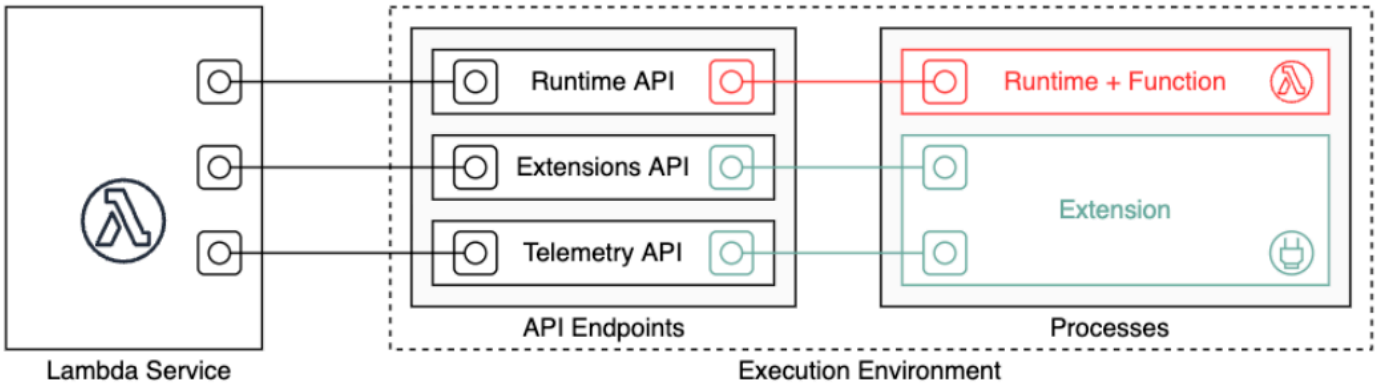
- 202 – Accepté
- 400 – Demande erronée.
- 403 – Interdit
- 500 — Erreur du conteneur. Non-recoverable état. L'extension doit se fermer rapidement.

Accès aux données de télémétrie en temps réel pour les extensions à l'aide de l'API de télémétrie

L'API de télémétrie active vos extensions pour recevoir directement des données de télémétrie de Lambda. Pendant l'initialisation et l'invocation des fonctions, Lambda capture automatiquement la télémétrie, notamment les journaux, les métriques de la plateforme et les traces de la plateforme. L'API de télémétrie active des extensions pour accéder à ces données de télémétrie directement depuis Lambda en temps quasi réel.

Dans l'environnement d'exécution Lambda, vous pouvez abonner vos extensions Lambda à des flux de télémétrie. Après la souscription, Lambda envoie automatiquement toutes les données de télémétrie à vos extensions. Vous pouvez ensuite traiter, filtrer et distribuer les données à votre destination préférée, telle qu'un compartiment Amazon Simple Storage Service (Amazon S3) ou un fournisseur d'outils d'observabilité tiers.

Le schéma suivant montre comment l'API d'extensions et l'API de télémétrie lient les extensions à Lambda depuis l'environnement d'exécution. En outre, l'API Runtime connecte votre environnement d'exécution et votre fonction d'événement à Lambda.



> **Important**
>
> L'API de télémétrie Lambda remplace l'API de journaux Lambda. Bien que l'API de journaux reste entièrement fonctionnelle, nous vous recommandons d'utiliser uniquement l'API de télémétrie à l'avenir. Vous pouvez abonner votre extension à un flux de télémétrie en utilisant l'API de télémétrie ou l'API de journaux. Après s'être abonné à l'aide de l'une de ces API, toute tentative d'abonnement à l'aide de l'autre API renvoie une erreur.

Exigence de version du schéma des instances gérées Lambda

Les instances gérées Lambda ne prennent en charge que la version du `2025-01-29` schéma de l'API de télémétrie. Lorsque vous vous abonnez à des flux de télémétrie pour les fonctions des instances gérées, vous devez les utiliser `"schemaVersion": "2025-01-29"` dans votre demande d'abonnement. L'utilisation de versions de schéma précédentes entraîne le rejet d'événements par Lambda.
La version du `2025-01-29` schéma est rétrocompatible et peut être utilisée à la fois avec les instances gérées Lambda et les fonctions Lambda (par défaut). Nous recommandons d'utiliser cette version pour toutes les nouvelles extensions afin de garantir la compatibilité entre les deux modèles de déploiement.

Les extensions peuvent utiliser l'API de télémétrie pour s'abonner à trois flux de télémétrie différents :

- Télémétrie de plateforme – Journaux, métriques et traces, qui décrivent les événements et les erreurs liés au cycle de vie de l'environnement d'exécution, au cycle de vie des extensions et aux appels de fonctions
- Journaux de fonctions : journaux personnalisés générés par le code de la fonction d'événement Lambda.
- Journaux d'extension – Journaux personnalisés générés par le code d'extension Lambda.

Note

Lambda envoie des journaux et des métriques et des traces à CloudWatch X-Ray (si vous avez activé le suivi), même si une extension est abonnée à des flux de télémétrie.

Sections

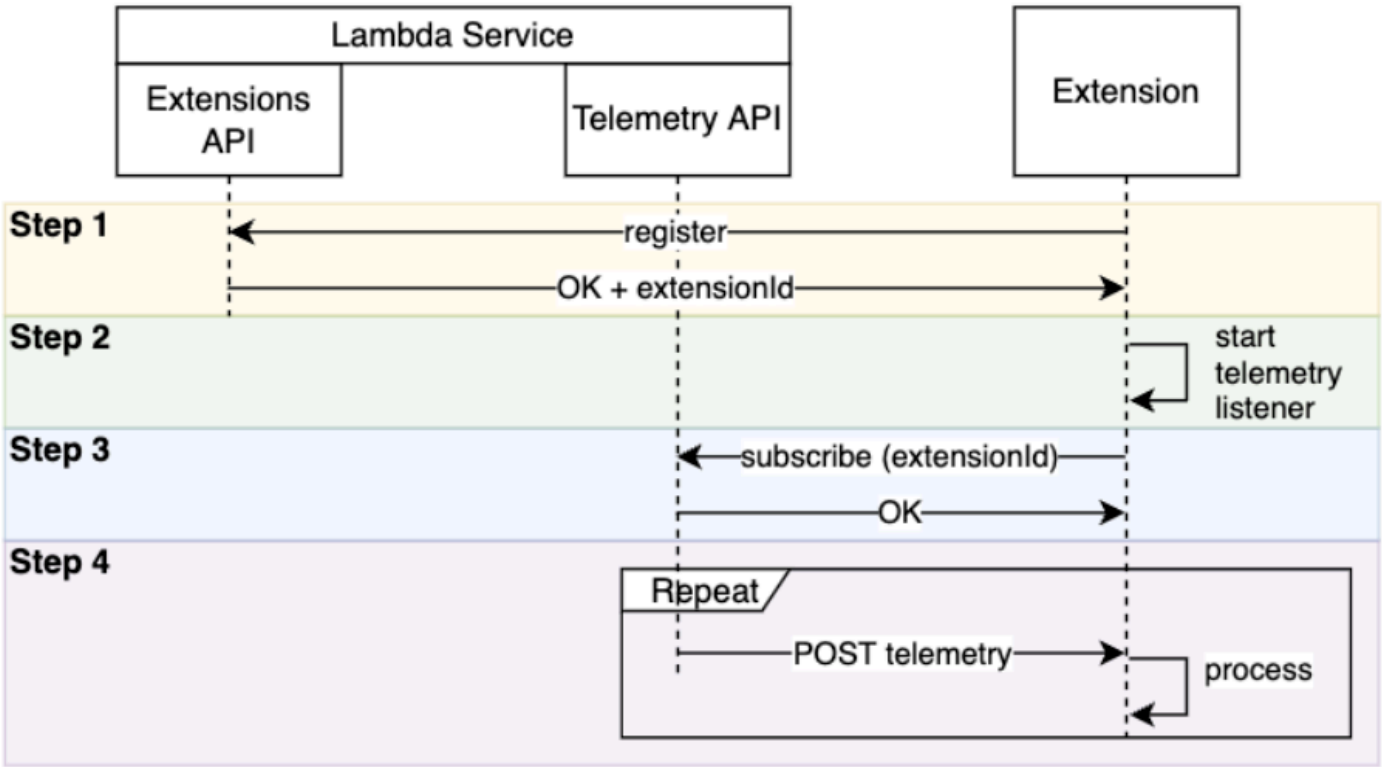
- Création d'extensions à l'aide de l'API de télémétrie
- Enregistrement de votre extension
- Création d'un écouteur de télémétrie
- Spécification d'un protocole de destination
- Configuration de l'utilisation de la mémoire et de la mise en mémoire tampon
- Envoi d'une demande d'abonnement à l'API de télémétrie

- Messages entrants de l’API de télémétrie
- Référence de l’API de télémétrie Lambda
- Référence du schéma d'événement de l'API de télémétrie Lambda
- Conversion des objets d'événements de l'API de télémétrie Lambda en spans OpenTelemetry
- Utilisation de l’API Logs Lambda

Création d’extensions à l’aide de l’API de télémétrie

Les extensions Lambda s’exécutent comme des processus indépendants dans l’environnement d’exécution. Les extensions peuvent continuer à s’exécuter une fois l’invocation des fonctions terminée. Comme les extensions sont des processus séparés, vous pouvez les écrire dans un langage différent du code de la fonction. Nous recommandons d’écrire les extensions en utilisant un langage compilé tel que Golang ou Rust. De cette façon, l’extension est un binaire autonome qui peut être compatible avec tout environnement d’exécution pris en charge.

Le schéma suivant illustre un processus en quatre étapes pour créer une extension qui reçoit et traite des données de télémétrie à l’aide de l’API de télémétrie.



Voici chaque étape plus en détail :

1. Enregistrez votre extension à l'aide du the section called "API d'extensions". Cela vous fournit un `Lambda-Extension-Identifier`, dont vous aurez besoin dans les étapes suivantes. Pour plus d'informations sur la façon d'enregistrer votre extension, consultez the section called "Enregistrement de votre extension".
2. Créez un écouteur de télémétrie. Il peut s'agir d'un serveur HTTP ou TCP de base. Lambda utilise l'URI de l'écouteur de télémétrie pour envoyer des données de télémétrie à votre extension. Pour plus d'informations, consultez the section called "Création d'un écouteur de télémétrie".
3. À l'aide de l'API d'abonnement de l'API de télémétrie, abonnez votre extension aux flux de télémétrie souhaités. Vous aurez besoin de l'URI de votre écouteur de télémétrie pour cette étape. Pour plus d'informations, consultez the section called "Envoi d'une demande d'abonnement à l'API de télémétrie".
4. Obtenez les données de télémétrie de Lambda via l'écouteur de télémétrie. Vous pouvez effectuer tout traitement personnalisé de ces données, par exemple en les envoyant vers Amazon S3 ou vers un service d'observabilité externe.

> **Note**
>
> L'environnement d'exécution d'une fonction événementielle peut démarrer et s'arrêter plusieurs fois au cours de son cycle de vie. En général, votre code d'extension s'exécute pendant les invocations de la fonction d'événement, et jusqu'à 2 secondes pendant la phase d'arrêt. Nous vous recommandons de regrouper la télémétrie au fur et à mesure qu'elle parvient à votre écouteur. Utilisez ensuite les événements du cycle de vie `Invoke` et `Shutdown` pour envoyer chaque lot vers les destinations souhaitées.

Enregistrement de votre extension

Avant de pouvoir vous abonner aux données de télémétrie, vous devez enregistrer votre extension Lambda. L'enregistrement a lieu pendant la phase d'initialisation de l'extension. L'exemple suivant montre une demande HTTP pour enregistrer une extension.

```
POST http://${AWS_LAMBDA_RUNTIME_API}/2020-01-01/extension/register
 Lambda-Extension-Name: lambda_extension_name
{
    'events': [ 'INVOKE', 'SHUTDOWN']
}
```

Si la demande réussit, l'abonné reçoit une réponse de succès HTTP 200. L'en-tête de réponse contient le `Lambda-Extension-Identifier`. Le corps de la réponse contient d'autres propriétés de la fonction.

```
HTTP/1.1 200 OK
Lambda-Extension-Identifier: a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
{
    "functionName": "lambda_function",
    "functionVersion": "$LATEST",
    "handler": "lambda_handler",
    "accountId": "123456789012"
}
```

Pour plus d'informations, consultez le the section called "Référence d'API d'extensions".

Création d'un écouteur de télémétrie

Votre extension Lambda doit avoir un écouteur qui traite les demandes entrantes de l'API de télémétrie. Le code suivant présente un exemple de mise en œuvre d'un écouteur de télémétrie en Golang :

```
// Starts the server in a goroutine where the log events will be sent
func (s *TelemetryApiListener) Start() (string, error) {
 address := listenOnAddress()
 l.Info("[listener:Start] Starting on address", address)
 s.httpServer = &http.Server{Addr: address}
 http.HandleFunc("/", s.http_handler)
 go func() {
  err := s.httpServer.ListenAndServe()
  if err != http.ErrServerClosed {
   l.Error("[listener:goroutine] Unexpected stop on Http Server:", err)
   s.Shutdown()
  } else {
   l.Info("[listener:goroutine] Http Server closed:", err)
  }
 }()
 return fmt.Sprintf("http://%s/", address), nil
}

// http_handler handles the requests coming from the Telemetry API.
// Everytime Telemetry API sends log events, this function will read them from the
 response body
```

```
// and put into a synchronous queue to be dispatched later.
// Logging or printing besides the error cases below is not recommended if you have
 subscribed to
// receive extension logs. Otherwise, logging here will cause Telemetry API to send new
 logs for
// the printed lines which may create an infinite loop.
func (s *TelemetryApiListener) http_handler(w http.ResponseWriter, r *http.Request) {
 body, err := ioutil.ReadAll(r.Body)
 if err != nil {
  l.Error("[listener:http_handler] Error reading body:", err)
  return
 }

 // Parse and put the log messages into the queue
 var slice []interface{}
 _ = json.Unmarshal(body, &slice)

 for _, el := range slice {
  s.LogEventsQueue.Put(el)
 }

 l.Info("[listener:http_handler] logEvents received:", len(slice), " LogEventsQueue
 length:", s.LogEventsQueue.Len())
 slice = nil
}
```

Spécification d’un protocole de destination

Lorsque vous vous abonnez pour recevoir de la télémétrie à l’aide de l’API de télémétrie, vous pouvez spécifier un protocole de destination en plus de l’URI de destination :

```
{
    "destination": {
        "protocol": "HTTP",
        "URI": "http://sandbox.localdomain:8080"
    }
}
```

Lambda accepte deux protocoles pour recevoir des télémétries :

- HTTP (recommandé) – Lambda envoie la télémétrie à un point de terminaison HTTP local (`http://sandbox.localdomain:${PORT}/${PATH}`) sous la forme d’un tableau

d'enregistrements au format JSON. Le paramètre `$PATH` est facultatif. Lambda ne prend en charge que HTTP, pas HTTPS. Lambda fournit des données de télémétrie via des demandes POST.

- TCP – Lambda envoie la télémétrie à un port TCP au format NDJSON (Newline delimited JSON).

> **Note**
>
> Nous vous recommandons vivement d'utiliser HTTP plutôt que TCP. Avec TCP, la plateforme Lambda ne peut pas confirmer la livraison de la télémétrie à la couche d'application. Par conséquent, si votre extension se bloque, vous risquez de perdre la télémétrie. HTTP ne présente pas cette limitation.

Avant de vous abonner pour recevoir la télémétrie, établissez l'écouteur HTTP local ou le port TCP. Au cours de l'installation, notez ce qui suit :

- Lambda n'envoie la télémétrie qu'à des destinations au sein de l'environnement d'exécution.
- Lambda réessaie d'envoyer la télémétrie (avec interruption) en l'absence d'écouteur, ou si la demande POST rencontre une erreur. Si l'écouteur de télémétrie se bloque, il reprend la réception de la télémétrie après que Lambda a redémarré l'environnement d'exécution.
- Lambda réserve le port 9001. Il n'y a pas d'autres restrictions ou recommandations relatives au numéro de port.

Configuration de l'utilisation de la mémoire et de la mise en mémoire tampon

L'utilisation de la mémoire dans un environnement d'exécution augmente de façon linéaire avec le nombre d'abonnés. Les abonnements consomment des ressources de mémoire, car chacun d'eux ouvre un nouveau tampon mémoire pour stocker les données de télémétrie. L'utilisation de la mémoire tampon contribue à la consommation globale de mémoire dans l'environnement d'exécution.

Lorsque vous vous abonnez pour recevoir des données télémétriques via l'API de télémétrie, vous pouvez mettre en mémoire tampon les données télémétriques et les transmettre aux abonnés par lots. Pour optimiser l'utilisation de la mémoire, vous pouvez spécifier une configuration de mise en mémoire tampon :

```
{
    "buffering": {
```

```
        "maxBytes": 256*1024,
        "maxItems": 1000,
        "timeoutMs": 100
    }
}
```

Paramètre	Description	Valeurs par défaut et limites
`maxBytes`	Le volume maximal de télémétrie (en octets) à mettre en mémoire tampon.	Par défaut : 262 144 Minimum : 262 144 Maximum : 1 048 576
`maxItems`	Le nombre maximal d'événements à mettre en mémoire tampon.	Par défaut : 10 000 Minimum : 1 000 Maximum : 10 000.
`timeoutMs`	La durée maximale (en millisecondes) pour la mise en mémoire tampon d'un lot.	Par défaut : 1 000 Minimum : 25 Maximum : 30 000

Lorsque vous configurez la mise en mémoire tampon, tenez compte des points suivants :

- Si l'un des flux d'entrée est fermé, Lambda vide les journaux. Cela peut se produire si, par exemple, l'environnement d'exécution se bloque.
- Chaque abonné peut spécifier une configuration de mise en mémoire tampon différente dans sa demande d'abonnement.
- Lorsque vous déterminez la taille de la mémoire tampon pour la lecture des données, attendez-vous à recevoir des charges utiles aussi importantes que `2 * maxBytes + metadataBytes`, `maxBytes` étant un composant de votre configuration de mise en mémoire tampon. Pour évaluer la quantité de `metadataBytes` à prendre en compte, consultez les métadonnées suivantes. Lambda adjoint des métadonnées similaires à celles-ci à chaque enregistrement :

```
{
```

```
    "time": "2022-08-20T12:31:32.123Z",
    "type": "function",
    "record": "Hello World"
}
```

- Si l'abonné ne parvient pas à traiter la télémétrie entrante assez rapidement, ou si votre code Event Function génère un volume de log très élevé, Lambda peut supprimer des enregistrements pour limiter l'utilisation de la mémoire. Lorsque cela se produit, Lambda envoie un événement `platform.logsDropped`.

Envoi d'une demande d'abonnement à l'API de télémétrie

Les extensions Lambda peuvent s'abonner pour recevoir des données de télémétrie en envoyant une demande d'abonnement à l'API de télémétrie. La demande d'abonnement doit contenir des informations sur les types d'événements auxquels vous voulez que l'extension s'abonne. En outre, la demande peut contenir des informations sur la destination de la livraison et une configuration de mise en mémoire tampon.

Avant d'envoyer une demande d'abonnement, vous devez disposer d'un ID d'extension (`Lambda-Extension-Identifier`). Lorsque vous enregistrez votre extension avec l'API d'extensions, vous obtenez un ID d'extension à partir de la réponse API.

L'abonnement a lieu pendant la phase d'initialisation de l'extension. L'exemple suivant montre une demande HTTP pour s'abonner aux trois flux de télémétrie : télémétrie de la plateforme, journaux des fonctions et journaux des extensions.

```
PUT http://${AWS_LAMBDA_RUNTIME_API}/2022-07-01/telemetry HTTP/1.1
{
   "schemaVersion": "2025-01-29",
   "types": [
        "platform",
        "function",
        "extension"
   ],
   "buffering": {
        "maxItems": 1000,
        "maxBytes": 256*1024,
        "timeoutMs": 100
   },
   "destination": {
        "protocol": "HTTP",
```

```
        "URI": "http://sandbox.localdomain:8080"
    }
}
```

Si la demande réussit, l'abonné reçoit une réponse de succès HTTP 200.

```
HTTP/1.1 200 OK
"OK"
```

Messages entrants de l'API de télémétrie

Après s'être abonnée à l'aide de l'API de télémétrie, une extension commence automatiquement à recevoir la télémétrie de Lambda via des requêtes POST. Chaque corps de requête POST contient un tableau d'objets `Event`. Chaque `Event` est structuré selon le schéma suivant :

```
{
   time: String,
   type: String,
   record: Object
}
```

- La propriété `time` définit le moment où la plateforme Lambda a généré l'événement. Cela est différent du moment où l'événement s'est réellement produit. La valeur de la chaîne `time` est un horodatage au format ISO 8601.
- La propriété `type` définit le type d'événement. Le tableau suivant décrit toutes les valeurs possibles.
- La propriété `record` définit un objet JSON qui contient les données de télémétrie. Le schéma de cet objet JSON dépend de la propriété `type`.

> **Commande d'événements avec invocations simultanées**
>
> Pour les instances gérées Lambda, plusieurs invocations de fonctions peuvent s'exécuter simultanément dans le même environnement d'exécution. Dans ce cas, l'ordre `platform.start` et les `platform.report` événements ne sont pas garantis entre les différentes invocations simultanées. Les extensions doivent gérer les événements issus de plusieurs invocations exécutées en parallèle et ne doivent pas adopter un ordre séquentiel. Pour attribuer correctement des événements à des invocations spécifiques, les extensions doivent utiliser le `requestId` champ présent dans ces événements de plateforme.

Chaque appel possède un identifiant de demande unique qui reste le même pour tous les événements associés à cet appel, ce qui permet aux extensions de corréler correctement les événements même lorsqu'ils arrivent dans le désordre.

Le tableau suivant résume tous les types d'objets `Event` et renvoie à la référence du schéma `Event` de l'API de télémétrie pour chaque type d'événement.

Catégorie	Type d'événement	Description	Schéma d'enregistrement des événements
Événement de plateforme	`platform.initStart`	L'initialisation de la fonction a commencé.	Schéma the section called "`Platform.initStart`"
Événement de plateforme	`platform.initRuntimeDone`	L'initialisation de la fonction est terminée.	Schéma the section called "`platform.init RuntimeDone`"
Événement de plateforme	`platform.initReport`	Un rapport d'initialisation de la fonction.	Schéma the section called "`Rapport Platform.init`"
Événement de plateforme	`platform.start`	L'invocation de la fonction a commencé.	Schéma the section called "`platform.start`"
Événement de plateforme	`platform.runtimeDone`	L'environnement d'exécution a fini de traiter un événement avec succès ou échec.	Schéma the section called "`platform.runtimeDone`"
Événement de plateforme	`platform.report`	Un rapport sur l'invocation de la fonction.	Schéma the section called "`platform.rapport`"

Catégorie	Type d'événement	Description	Schéma d'enregistrement des événements
Événement de plateforme	`platform.restoreStart`	La restauration de l'exécution a commencé.	Schéma the section called "`Platform.restoRestart`"
Événement de plateforme	`platform.restoreRuntimeDone`	La restauration de l'exécution est terminée.	Schéma the section called "`platform.restore RuntimeDone`"
Événement de plateforme	`platform.restoreReport`	Le rapport de restauration de d'exécution.	Schéma the section called "`Platform.RestoreReport`"
Événement de plateforme	`platform.telemetrySubscription`	L'extension s'est abonnée à l'API de télémétrie.	Schéma the section called "`Plateforme.Abonnement à la télémétrie`"
Événement de plateforme	`platform.logsDropped`	Les entrées de journal abandonnées par Lambda.	Schéma the section called "`Plate-forme. LogsDropped`"
Journaux de fonctions	`function`	Une ligne de journal du code de la fonction.	Schéma the section called "`fonction`"
Journaux d'extension	`extension`	Une ligne de journal du code de l'extension.	Schéma the section called "`Extension`"

Référence de l'API de télémétrie Lambda

Utilisez le point de terminaison de l'API de télémétrie Lambda pour abonner des extensions aux flux de télémétrie. Vous pouvez extraire le point de terminaison d'API de télémétrie à partir de la variable d'environnement `AWS_LAMBDA_RUNTIME_API`. Pour envoyer une demande d'API, ajoutez la version de l'API (`2022-07-01/`) et `telemetry/`. Par exemple :

```
http://${AWS_LAMBDA_RUNTIME_API}/2022-07-01/telemetry/
```

Pour la définition de la spécification OpenAPI (OAS) de la version des réponses d'abonnement `2025-01-29`, voir ce qui suit :

- HTTP — telemetry-api-http-schema.zip
- TCP — .zip telemetry-api-tcp-schema

Opérations d'API

- S'abonner

S'abonner

Pour s'abonner à un flux de télémétrie, une extension Lambda peut envoyer une demande d'API d'abonnement.

- Chemin – `/telemetry`
- Méthode – PUT
- En-têtes
  - `Content-Type`: `application/json`
- Paramètres du corps de la demande
  - schemaVersion
    - Obligatoire : oui
    - Type : String
    - Valeurs valides : `"2025-01-29"`, `"2022-12-13"` ou `"2022-07-01"`
    - Remarque : les instances gérées Lambda nécessitent. `"2025-01-29"` Cette version est rétrocompatible avec les fonctions Lambda (par défaut).

- destination – Les paramètres de configuration qui définissent la destination de l'événement de télémétrie et le protocole de livraison de l'événement.
  - Obligatoire : oui
  - Type : objet

```
{
    "protocol": "HTTP",
    "URI": "http://sandbox.localdomain:8080"
}
```

  - protocol – Le protocole que Lambda utilise pour envoyer les données de télémétrie.
    - Obligatoire : oui
    - Type : String
    - Valeurs valides : `"HTTP"|"TCP"`
  - URI – L'URI auquel envoyer les données de télémétrie.
    - Obligatoire : oui
    - Type : String
  - Pour de plus amples informations, veuillez consulter the section called "Spécification d'un protocole de destination".
- types – Les types de télémétrie auxquels vous voulez que l'extension s'abonne.
  - Obligatoire : oui
  - Type : tableau de chaînes
  - Valeurs valides : `"platform"|"function"|"extension"`
- buffering – Les paramètres de configuration de la mise en mémoire tampon des événements.
  - Obligatoire : non
  - Type : objet

```
{
   "buffering": {
        "maxItems": 1000,
        "maxBytes": 256*1024,
        "timeoutMs": 100
   }
}
```


    - maxItems – Nombre maximum d'événements à mettre en mémoire tampon.

    - Obligatoire : non
    - Type : Integer
    - Par défaut : 1 000
    - Minimum : 1 000
    - Maximum : 10 000.
- maxBytes – Le volume maximal de télémétrie (en octets) à mettre en mémoire tampon.
    - Obligatoire : non
    - Type : Integer
    - Par défaut : 262 144
    - Minimum : 262 144
    - Maximum : 1 048 576
- timeoutMs – Durée maximum (en millisecondes) de mise en mémoire tampon d'un lot.
    - Obligatoire : non
    - Type : Integer
    - Par défaut : 1 000
    - Minimum : 25
    - Maximum : 30 000
- Pour de plus amples informations, veuillez consulter the section called "Configuration de l'utilisation de la mémoire et de la mise en mémoire tampon".

Exemple de demande d'API d'abonnement

```
PUT http://${AWS_LAMBDA_RUNTIME_API}/2022-07-01/telemetry HTTP/1.1
{
   "schemaVersion": "2025-01-29",
   "types": [
        "platform",
        "function",
        "extension"
   ],
   "buffering": {
        "maxItems": 1000,
        "maxBytes": 256*1024,
        "timeoutMs": 100
   },
```

```
   "destination": {
        "protocol": "HTTP",
        "URI": "http://sandbox.localdomain:8080"
   }
}
```

Si la demande d'abonnement aboutit, l'extension reçoit une réponse HTTP 200 :

```
HTTP/1.1 200 OK
"OK"
```

Si la demande d'abonnement échoue, l'extension reçoit une réponse d'erreur. Par exemple :

```
HTTP/1.1 400 OK
{
    "errorType": "ValidationError",
    "errorMessage": "URI port is not provided; types should not be empty"
}
```

Voici quelques codes de réponse supplémentaires que l'extension peut recevoir :

- 200 – Demande effectuée avec succès.
- 202 – Demande acceptée. Réponse à une demande d'abonnement dans un environnement de test local
- 400 – Demande erronée
- 500 – Erreur de service.

Référence du schéma d'événement de l'API de télémétrie Lambda

Utilisez le point de terminaison de l'API de télémétrie Lambda pour abonner des extensions aux flux de télémétrie. Vous pouvez extraire le point de terminaison d'API de télémétrie à partir de la variable d'environnement `AWS_LAMBDA_RUNTIME_API`. Pour envoyer une demande d'API, ajoutez la version de l'API (`2022-07-01/`) et `telemetry/`. Par exemple :

```
http://${AWS_LAMBDA_RUNTIME_API}/2022-07-01/telemetry/
```

Pour la définition de la spécification OpenAPI (OAS) de la version des réponses d'abonnement `2025-01-29`, voir ce qui suit :

- HTTP – telemetry-api-http-schema.zip
- TCP – telemetry-api-tcp-schema.zip

Le tableau suivant est un résumé de tous les types d'objets `Event` que l'API de télémétrie prend en charge.

Catégorie	Type d'événement	Description	Schéma d'enregistrement des événements
Événement de plateforme	`platform.initStart`	L'initialisation de la fonction a commencé.	Schéma the section called "`Platform.initStart`"
Événement de plateforme	`platform.initRuntimeDone`	L'initialisation de la fonction est terminée.	Schéma the section called "`platform.initRuntimeDone`"
Événement de plateforme	`platform.initReport`	Un rapport d'initialisation de la fonction.	Schéma the section called "`Rapport Platform.init`"

Catégorie	Type d'événement	Description	Schéma d'enregistrement des événements
Événement de plateforme	`platform.start`	L'invocation de la fonction a commencé.	Schéma the section called "`platform.start`"
Événement de plateforme	`platform.runtimeDone`	L'environnement d'exécution a fini de traiter un événement avec succès ou échec.	Schéma the section called "`platform.runtimeDone`"
Événement de plateforme	`platform.report`	Un rapport sur l'invocation de la fonction.	Schéma the section called "`platform.rapport`"
Événement de plateforme	`platform.restoreStart`	La restauration de l'exécution a commencé.	Schéma the section called "`Platform.restoRestart`"
Événement de plateforme	`platform.restoreRuntimeDone`	La restauration de l'exécution est terminée.	Schéma the section called "`platform.restore RuntimeDone`"
Événement de plateforme	`platform.restoreReport`	Le rapport de restauration de d'exécution.	Schéma the section called "`Platform.RestoreReport`"
Événement de plateforme	`platform.telemetrySubscription`	L'extension s'est abonnée à l'API de télémétrie.	Schéma the section called "`Plateforme.Abonnement à la télémétrie`"

Catégorie	Type d'événement	Description	Schéma d'enregistrement des événements
Événement de plateforme	`platform.logsDropped`	Les entrées de journal abandonnées par Lambda.	Schéma the section called "`Plate-forme. LogsDropped`"
Journaux de fonctions	`function`	Une ligne de journal du code de la fonction.	Schéma the section called "`fonction`"
Journaux d'extension	`extension`	Une ligne de journal du code de l'extension.	Schéma the section called "`Extension`"

Table des matières

- Types d'objets d'événements de l'API de télémétrie
  - Platform.initStart
  - platform.init RuntimeDone
  - Rapport Platform.init
  - platform.start
  - platform.runtimeDone
  - platform.rapport
  - Platform.restoRestart
  - platform.restore RuntimeDone
  - Platform.RestoreReport
  - plate-forme.extension
  - Plateforme.Abonnement à la télémétrie
  - Plate-forme. LogsDropped
  - fonction
  - Extension

- Types d’objets partagés
  - InitPhase
  - InitReportMetrics
  - InitType
  - ReportMetrics
  - RestoreReportMetrics
  - RuntimeDoneMetrics
  - Span
  - Statut
  - TraceContext
  - TracingType

Types d'objets d'**`événements`** de l'API de télémétrie

Cette section détaille les types d’objets `Event` que l’API de télémétrie Lambda prend en charge. Dans les descriptions d’événements, un point d’interrogation (?) indique que l’attribut peut ne pas être présent dans l’objet.

`Platform.initStart`

Un `platform.initStart` événement indique que la phase d'initialisation de la fonction d'événement a commencé. Un objet `Event` `platform.initStart` a la forme suivante :

```
Event: Object
- time: String
- type: String = platform.initStart
- record: PlatformInitStart
```

L’objet `PlatformInitStart` possède les attributs suivants :

- functionName – `String`
- functionVersion – `String`
- InitializationType – Objet `the section called “InitType”`
- instanceId? – `String`
- un exemple MaxMemory ? — `Integer`

- phase – Objet the section called “InitPhase”
- runtimeVersion? – String
- durée d'exécution VersionArn ? — String

Voici un exemple de Event de type platform.initStart :

```
{
    "time": "2022-10-12T00:00:15.064Z",
    "type": "platform.initStart",
    "record": {
        "initializationType": "on-demand",
        "phase": "init",
        "runtimeVersion": "nodejs-14.v3",
        "runtimeVersionArn": "arn",
        "functionName": "myFunction",
        "functionVersion": "$LATEST",
        "instanceId": "82561ce0-53dd-47d1-90e0-c8f5e063e62e",
        "instanceMaxMemory": 256
    }
}
```

platform.init RuntimeDone

Un platform.initRuntimeDone événement indique que la phase d'initialisation de la fonction d'événement est terminée. Un objet Event platform.initRuntimeDone a la forme suivante :

```
Event: Object
- time: String
- type: String = platform.initRuntimeDone
- record: PlatformInitRuntimeDone
```

L’objet PlatformInitRuntimeDone possède les attributs suivants :

- InitializationType – Objet the section called “InitType”
- phase – Objet the section called “InitPhase”
- status – Objet the section called “Statut”
- spans? – Liste d’objets the section called “Span”

Voici un exemple de Event de type platform.initRuntimeDone :

```
{
    "time": "2022-10-12T00:01:15.000Z",
    "type": "platform.initRuntimeDone",
    "record": {
        "initializationType": "on-demand"
        "status": "success",
        "spans": [
            {
                "name": "someTimeSpan",
                "start": "2022-06-02T12:02:33.913Z",
                "durationMs": 70.5
            }
        ]
    }
}
```

Rapport Platform.init

Un `platform.initReport` événement contient un rapport global de la phase d'initialisation de la fonction d'événement. Un objet `Event` `platform.initReport` a la forme suivante :

```
Event: Object
- time: String
- type: String = platform.initReport
- record: PlatformInitReport
```

L'objet `PlatformInitReport` possède les attributs suivants :

- errorType? – chaîne
- InitializationType – Objet the section called "InitType"
- phase – Objet the section called "InitPhase"
- metrics – Objet the section called "InitReportMetrics"
- spans? – Liste d'objets the section called "Span"
- status – Objet the section called "Statut"

Voici un exemple de `Event` de type `platform.initReport` :

```
{
    "time": "2022-10-12T00:01:15.000Z",
```

```
    "type": "platform.initReport",
    "record": {
        "initializationType": "on-demand",
        "status": "success",
        "phase": "init",
        "metrics": {
            "durationMs": 125.33
        },
        "spans": [
            {
                "name": "someTimeSpan",
                "start": "2022-06-02T12:02:33.913Z",
                "durationMs": 90.1
            }
        ]
    }
}
```

`platform.start`

Un `platform.start` événement indique que la phase d'invocation de la fonction d'événement a commencé. Un objet `Event` `platform.start` a la forme suivante :

```
Event: Object
- time: String
- type: String = platform.start
- record: PlatformStart
```

L'objet `PlatformStart` possède les attributs suivants :

- requestId – `String`
- version? – `String`
- tracing? – the section called "TraceContext"

Voici un exemple de `Event` de type `platform.start` :

```
{
    "time": "2022-10-12T00:00:15.064Z",
    "type": "platform.start",
    "record": {
        "requestId": "6d68ca91-49c9-448d-89b8-7ca3e6dc66aa",
```

```
        "version": "$LATEST",
        "tracing": {
            "spanId": "54565fb41ac79632",
            "type": "X-Amzn-Trace-Id",
            "value":
 "Root=1-62e900b2-710d76f009d6e7785905449a;Parent=0efbd19962d95b05;Sampled=1"
        }
    }
}
```

`platform.runtimeDone`

Un `platform.runtimeDone` événement indique que la phase d'invocation de la fonction d'événement est terminée. Un objet `Event` `platform.runtimeDone` a la forme suivante :

> **Instances gérées par Lambda**
>
> L'`platform.runtimeDone`événement n'est pas pris en charge pour les instances gérées Lambda. Les extensions exécutées sur les instances gérées ne reçoivent pas cet événement car les extensions ne peuvent pas s'abonner à l'`INVOKE`événement sur les instances gérées. En raison du modèle d'exécution simultanée dans lequel plusieurs invocations peuvent être traitées simultanément, les extensions ne peuvent pas effectuer de traitement post-appel pour des invocations individuelles comme elles le font traditionnellement sur les fonctions Lambda (par défaut).
>
> Pour les instances gérées, les `responseLatency` intervalles `responseDuration` et qui y sont normalement inclus `platform.runtimeDone` sont plutôt disponibles lors de l'`platform.report`événement. Consultez the section called “`platform.rapport`” pour plus de détails.

```
Event: Object
- time: String
- type: String = platform.runtimeDone
- record: PlatformRuntimeDone
```

L’objet `PlatformRuntimeDone` possède les attributs suivants :

- errorType? – `String`
- metrics? – Objet the section called “RuntimeDoneMetrics”

- requestId – `String`
- status – Objet the section called “Statut”
- spans? – Liste d’objets the section called “Span”
- tracing? – Objet the section called “TraceContext”

Voici un exemple de `Event` de type `platform.runtimeDone` :

```
{
    "time": "2022-10-12T00:01:15.000Z",
    "type": "platform.runtimeDone",
    "record": {
        "requestId": "6d68ca91-49c9-448d-89b8-7ca3e6dc66aa",
        "status": "success",
        "tracing": {
            "spanId": "54565fb41ac79632",
            "type": "X-Amzn-Trace-Id",
            "value":
 "Root=1-62e900b2-710d76f009d6e7785905449a;Parent=0efbd19962d95b05;Sampled=1"
        },
        "spans": [
            {
                "name": "someTimeSpan",
                "start": "2022-08-02T12:01:23:521Z",
                "durationMs": 80.0
            }
        ],
        "metrics": {
            "durationMs": 140.0,
            "producedBytes": 16
        }
    }
}
```

`platform.rapport`

Un `platform.report` événement contient un rapport global de la phase d'appel de la fonction d'événement. Un objet `Event` `platform.report` a la forme suivante :

Instances gérées par Lambda

L'`platform.report`événement pour les instances gérées Lambda a des métriques et des durées différentes par rapport aux fonctions Lambda (par défaut). Pour les instances gérées :

- Portée : contient `responseLatency` et `responseDuration` au lieu de. `extensionOverhead` L'`extensionOverhead`intervalle n'est pas disponible car les extensions ne peuvent pas s'abonner à l'`INVOKE`événement sur les instances gérées en raison du modèle d'exécution simultanée.
- Métriques : inclut uniquement`durationMs`. Les mesures suivantes ne sont pas incluses : `billedDurationMs`,`initDurationMs`,`maxMemoryUsedMB`, et`memorySizeMB`. Ces métriques par appel ne sont pas applicables dans l'environnement d'exécution simultanée. Pour les mesures d'utilisation des ressources, utilisez Surveillance des instances gérées Lambda Lambda Insights.

```
Event: Object
- time: String
- type: String = platform.report
- record: PlatformReport
```

L'objet `PlatformReport` possède les attributs suivants :

- metrics – Objet `the section called "ReportMetrics"`
- requestId – `String`
- spans? – Liste d'objets `the section called "Span"`
- status – Objet `the section called "Statut"`
- tracing? – Objet `the section called "TraceContext"`

Voici un exemple de `Event` de type `platform.report` :

```
{
    "time": "2022-10-12T00:01:15.000Z",
    "type": "platform.report",
    "record": {
        "metrics": {
            "billedDurationMs": 694,
```

```
            "durationMs": 693.92,
            "initDurationMs": 397.68,
            "maxMemoryUsedMB": 84,
            "memorySizeMB": 128
        },
        "requestId": "6d68ca91-49c9-448d-89b8-7ca3e6dc66aa",
    }
}
```

`Platform.restoRestart`

Un `platform.restoreStart` événement indique qu'un événement de restauration de l'environnement Event Function a commencé. Dans un événement de restauration d'environnement, Lambda crée l'environnement à partir d'un instantané mis en cache plutôt que de l'initialiser à partir de zéro. Pour plus d'informations, consultez SnapStart. Un objet `Event` `platform.restoreStart` a la forme suivante :

```
Event: Object
- time: String
- type: String = platform.restoreStart
- record: PlatformRestoreStart
```

L'objet `PlatformRestoreStart` possède les attributs suivants :

- functionName – `String`
- functionVersion – `String`
- instanceId? – `String`
- un exemple MaxMemory ? — `String`
- runtimeVersion? – `String`
- durée d'exécution VersionArn ? — `String`

Voici un exemple de `Event` de type `platform.restoreStart` :

```
{
    "time": "2022-10-12T00:00:15.064Z",
    "type": "platform.restoreStart",
    "record": {
        "runtimeVersion": "nodejs-14.v3",
        "runtimeVersionArn": "arn",
```

```
        "functionName": "myFunction",
        "functionVersion": "$LATEST",
        "instanceId": "82561ce0-53dd-47d1-90e0-c8f5e063e62e",
        "instanceMaxMemory": 256
    }
}
```

`platform.restore RuntimeDone`

Un `platform.restoreRuntimeDone` événement indique qu'un événement de restauration de l'environnement Event Function est terminé. Dans un événement de restauration d'environnement, Lambda crée l'environnement à partir d'un instantané mis en cache plutôt que de l'initialiser à partir de zéro. Pour plus d'informations, consultez SnapStart. Un objet `Event` `platform.restoreRuntimeDone` a la forme suivante :

```
Event: Object
- time: String
- type: String = platform.restoreRuntimeDone
- record: PlatformRestoreRuntimeDone
```

L'objet `PlatformRestoreRuntimeDone` possède les attributs suivants :

- errorType? – `String`
- spans? – Liste d'objets `the section called "Span"`
- status – Objet `the section called "Statut"`

Voici un exemple de `Event` de type `platform.restoreRuntimeDone` :

```
{
    "time": "2022-10-12T00:00:15.064Z",
    "type": "platform.restoreRuntimeDone",
    "record": {
        "status": "success",
        "spans": [
            {
                "name": "someTimeSpan",
                "start": "2022-08-02T12:01:23:521Z",
                "durationMs": 80.0
            }
        ]
```

```
    }
}
```

`Platform.RestoreReport`

Un `platform.restoreReport` événement contient un rapport global d'un événement de restauration d'une fonction événementielle. Un objet `Event` `platform.restoreReport` a la forme suivante :

```
Event: Object
- time: String
- type: String = platform.restoreReport
- record: PlatformRestoreReport
```

L'objet `PlatformRestoreReport` possède les attributs suivants :

- errorType? – chaîne
- metrics? – Objet the section called "RestoreReportMetrics"
- spans? – Liste d'objets the section called "Span"
- status – Objet the section called "Statut"

Voici un exemple de `Event` de type `platform.restoreReport` :

```
{
    "time": "2022-10-12T00:00:15.064Z",
    "type": "platform.restoreReport",
    "record": {
        "status": "success",
        "metrics": {
            "durationMs": 15.19
        },
        "spans": [
            {
                "name": "someTimeSpan",
                "start": "2022-08-02T12:01:23:521Z",
                "durationMs": 30.0
            }
        ]
    }
}
```

plate-forme.extension

Un événement `extension` contient des journaux provenant du code d'extension. Un objet `Event` `extension` a la forme suivante :

```
Event: Object
- time: String
- type: String = extension
- record: {}
```

L'objet `PlatformExtension` possède les attributs suivants :

- events – Liste de `String`
- nom – `String`
- state – `String`

Voici un exemple de `Event` de type `platform.extension` :

```
{
    "time": "2022-10-12T00:02:15.000Z",
    "type": "platform.extension",
    "record": {
        "events": [ "INVOKE", "SHUTDOWN" ],
        "name": "my-telemetry-extension",
        "state": "Ready"
    }
}
```

Plateforme.Abonnement à la télémétrie

Un événement `platform.telemetrySubscription` contient des informations sur un abonnement d'extension. Un objet `Event` `platform.telemetrySubscription` a la forme suivante :

```
Event: Object
- time: String
- type: String = platform.telemetrySubscription
- record: PlatformTelemetrySubscription
```

L'objet `PlatformTelemetrySubscription` possède les attributs suivants :

- nom – `String`
- state – `String`
- types – Liste de `String`

Voici un exemple de `Event` de type `platform.telemetrySubscription` :

```
{
    "time": "2022-10-12T00:02:35.000Z",
    "type": "platform.telemetrySubscription",
    "record": {
        "name": "my-telemetry-extension",
        "state": "Subscribed",
        "types": [ "platform", "function" ]
    }
}
```

Plate-forme. LogsDropped

Un événement `platform.logsDropped` contient des informations sur les événements abandonnés. Lambda émet l'`platform.logsDropped`événement lorsqu'une fonction d'événement produit des logs à un débit trop élevé pour que Lambda puisse les traiter. Lorsque Lambda ne parvient pas à envoyer des journaux vers CloudWatch ou vers l'extension abonnée à l'API de télémétrie au rythme où la fonction d'événement les produit, il supprime les journaux pour empêcher l'exécution de la fonction d'événement de ralentir. Un objet `Event` `platform.logsDropped` a la forme suivante :

```
Event: Object
- time: String
- type: String = platform.logsDropped
- record: PlatformLogsDropped
```

L'objet `PlatformLogsDropped` possède les attributs suivants :

- droppedBytes – `Integer`
- droppedRecords – `Integer`
- reason – `String`

Voici un exemple de `Event` de type `platform.logsDropped` :

```
{
    "time": "2022-10-12T00:02:35.000Z",
    "type": "platform.logsDropped",
    "record": {
        "droppedBytes": 12345,
        "droppedRecords": 123,
        "reason": "Some logs were dropped because the downstream consumer is slower
 than the logs production rate"
    }
}
```

`fonction`

Un `function` événement contient des journaux issus du code de la fonction d'événement. Un objet `Event` `function` a la forme suivante :

```
Event: Object
- time: String
- type: String = function
- record: {}
```

Le format du `record` champ varie selon que les journaux de votre fonction d'événement sont formatés en texte brut ou au format JSON. Pour en savoir plus sur les options de configuration du format de journal, voir the section called “Formats des journaux”

Voici un exemple `Event` de type `function` où le format du journal est en texte brut :

```
{
    "time": "2022-10-12T00:03:50.000Z",
    "type": "function",
    "record": "[INFO] Hello world, I am a function!"
}
```

Voici un exemple `Event` de type `function` où le journal est au format JSON :

```
{
    "time": "2022-10-12T00:03:50.000Z",
    "type": "function",
    "record": {
        "timestamp": "2022-10-12T00:03:50.000Z",
```

```
        "level": "INFO",
        "requestId": "79b4f56e-95b1-4643-9700-2807f4e68189",
        "message": "Hello world, I am a function!"
    }
}
```

> **Note**
>
> Si la version du schéma que vous utilisez est plus ancienne que la `2022-12-13` version, elle `"record"` est toujours affichée sous forme de chaîne, même lorsque le format de journalisation de votre fonction d'événement est configuré au format JSON. Pour les instances gérées Lambda, vous devez utiliser la version du schéma. `2025-01-29`

`Extension`

Un événement `extension` contient des journaux provenant du code d'extension. Un objet `Event` `extension` a la forme suivante :

```
Event: Object
- time: String
- type: String = extension
- record: {}
```

Le format du `record` champ varie selon que les journaux de votre fonction d'événement sont formatés en texte brut ou au format JSON. Pour en savoir plus sur les options de configuration du format de journal, voir the section called “Formats des journaux”

Voici un exemple `Event` de type `extension` où le format du journal est en texte brut :

```
{
    "time": "2022-10-12T00:03:50.000Z",
    "type": "extension",
    "record": "[INFO] Hello world, I am an extension!"
}
```

Voici un exemple `Event` de type `extension` où le journal est au format JSON :

```
{
```

```
    "time": "2022-10-12T00:03:50.000Z",
    "type": "extension",
    "record": {
       "timestamp": "2022-10-12T00:03:50.000Z",
       "level": "INFO",
       "requestId": "79b4f56e-95b1-4643-9700-2807f4e68189",
       "message": "Hello world, I am an extension!"
    }
}
```

> **Note**
>
> Si la version du schéma que vous utilisez est plus ancienne que la `2022-12-13` version, elle `"record"` est toujours affichée sous forme de chaîne, même lorsque le format de journalisation de votre fonction d'événement est configuré au format JSON. Pour les instances gérées Lambda, vous devez utiliser la version du schéma. `2025-01-29`

Types d'objets partagés

Cette section détaille les types d'objets partagés que l'API de télémétrie Lambda prend en charge.

`InitPhase`

Une enum de chaînes de caractères qui décrit la phase où l'étape d'initialisation se produit. Dans la plupart des cas, Lambda exécute le code d'initialisation de la fonction d'événement pendant la phase. `init` Toutefois, dans certains cas d'erreur, Lambda peut réexécuter le code d'initialisation de la fonction d'événement au cours de la phase. `invoke` (Cela s'appelle une init supprimée.)

- Type – `String`
- Valeurs valides : `init|invoke|snap-start`

`InitReportMetrics`

Un objet qui contient des métriques sur une phase d'initialisation.

- Type – `Object`

Un objet `InitReportMetrics` a la forme suivante :

```
InitReportMetrics: Object
- durationMs: Double
```

Voici un exemple d'objet `InitReportMetrics` :

```
{
    "durationMs": 247.88
}
```

`InitType`

Une enum de chaînes de caractères qui décrit comment Lambda a initialisé l'environnement.

- Type – `String`
- Valeurs valides – `on-demand`|`provisioned-concurrency`

`ReportMetrics`

Un objet qui contient des métriques sur une phase terminée.

- Type – `Object`

Un objet `ReportMetrics` a la forme suivante :

```
ReportMetrics: Object
- billedDurationMs: Integer
- durationMs: Double
- initDurationMs?: Double
- maxMemoryUsedMB: Integer
- memorySizeMB: Integer
- restoreDurationMs?: Double
```

Voici un exemple d'objet `ReportMetrics` :

```
{
    "billedDurationMs": 694,
    "durationMs": 693.92,
    "initDurationMs": 397.68,
    "maxMemoryUsedMB": 84,
```

```
    "memorySizeMB": 128
}
```

`RestoreReportMetrics`

Un objet qui contient des métriques sur une phase de restauration terminée.

- Type – `Object`

Un objet `RestoreReportMetrics` a la forme suivante :

```
RestoreReportMetrics: Object
- durationMs: Double
```

Voici un exemple d'objet `RestoreReportMetrics` :

```
{
    "durationMs": 15.19
}
```

`RuntimeDoneMetrics`

Un objet qui contient des métriques sur une phase d'invocation.

- Type – `Object`

Un objet `RuntimeDoneMetrics` a la forme suivante :

```
RuntimeDoneMetrics: Object
- durationMs: Double
- producedBytes?: Integer
```

Voici un exemple d'objet `RuntimeDoneMetrics` :

```
{
    "durationMs": 200.0,
    "producedBytes": 15
}
```

Span

Un objet qui contient des détails sur un span. Un span représente une unité de travail ou une opération dans une trace. Pour plus d'informations sur les spans, consultez Span sur la page de l'API de suivi du site Web de OpenTelemetry Docs.

Lambda prend en charge les span suivants pour l'événement `platform.RuntimeDone` :

- Le `responseLatency` span décrit le temps qu'il a fallu à votre fonction d'événement Lambda pour commencer à envoyer la réponse.
- Le `responseDuration` span décrit le temps qu'il a fallu à votre fonction d'événement Lambda pour terminer l'envoi de la réponse complète.
- Le `runtimeOverhead` span décrit le temps qu'il a fallu au moteur d'exécution Lambda pour signaler qu'il était prêt à traiter le prochain appel de la fonction d'événement. C'est le temps qu'il a fallu au moteur d'exécution pour appeler l'API d'invocation suivante afin d'obtenir le prochain événement après avoir renvoyé votre réponse Event Function.

Voici un exemple d'objet span `responseLatency` :

```
{
        "name": "responseLatency",
        "start": "2022-08-02T12:01:23.521Z",
        "durationMs": 23.02
      }
```

Statut

Un objet qui décrit le statut d'une phase d'initialisation ou d'invocation. Si le statut est `failure` ou `error`, l'objet `Status` contient également un champ `errorType` décrivant l'erreur.

- Type – `Object`
- Valeurs de status valides : `success`|`failure`|`error`|`timeout`

TraceContext

Un objet qui décrit les propriétés d'une trace.

- Type – `Object`

Un objet `TraceContext` a la forme suivante :

```
TraceContext: Object
- spanId?: String
- type: TracingType enum
- value: String
```

Voici un exemple d'objet `TraceContext` :

```
{
    "spanId": "073a49012f3c312e",
    "type": "X-Amzn-Trace-Id",
    "value":
 "Root=1-62e900b2-710d76f009d6e7785905449a;Parent=0efbd19962d95b05;Sampled=1"
}
```

`TracingType`

Un enum de chaînes de caractères qui décrit le type de trace dans un objet the section called "TraceContext".

- Type – `String`
- Valeurs valides – `X-Amzn-Trace-Id`

Conversion des objets d'événements de l'API de télémétrie Lambda en spans OpenTelemetry

Le schéma de l'API AWS Lambda de télémétrie est sémantiquement compatible avec OpenTelemetry (OTel). Cela signifie que vous pouvez convertir les `Event` objets de votre API de AWS Lambda télémétrie en OpenTelemetry (OTel) Spans. Lors de la conversion, vous ne devez pas mapper un seul objet `Event` à un seul OTel Span.

Au lieu de cela, vous devez présenter les trois événements liés à une phase du cycle de vie dans un seul OTel Span. Par exemple, les `runtimeReport` événements `startruntimeDone`, et représentent une seule invocation d'une fonction d'événement. Présentez ces trois événements sous la forme d'un seul OTel Span.

Vous pouvez convertir vos événements en utilisant des événements Span ou des Spans enfants (imbriqués). Les tableaux de cette page décrivent les mappages entre les propriétés du schéma de l'API de télémétrie et les propriétés des OTel Spans pour les deux approches. Pour plus d'informations sur OTel Spans, consultez Span sur la page de l'API de suivi du site Web de OpenTelemetry Docs.

Sections

- Mappage vers les OTel Spans avec les événements Span
- Mappage vers des OTel Spans avec des Spans enfants

Mappage vers les OTel Spans avec les événements Span

Dans les tableaux suivants, e représente l'événement provenant de la source de télémétrie.

Mappage des événements *Start

OpenTelemetry	Schéma de l'API de télémétrie Lambda
`Span.Name`	Votre extension génère cette valeur sur la base du champ `type`.
`Span.StartTime`	Utilisez `e.time`.
`Span.EndTime`	N/A, car l'événement n'est pas encore terminé.
`Span.Kind`	Définie sur `Server`.

OpenTelemetry	Schéma de l'API de télémétrie Lambda
`Span.Status`	Définie sur `Unset`.
`Span.TraceId`	Analysez l' AWS X-Ray en-tête trouvé dans `.tracing.value` , puis utilisez la `TraceId` valeur.
`Span.ParentId`	Analysez l' X-Ray en-tête trouvé dans `.tracing.value` , puis utilisez la `Parent` valeur.
`Span.SpanId`	Utilisez `e.tracing.spanId` si disponible. Sinon, générer un nouveau `SpanId`.
`Span.SpanContext.TraceState`	N/A pour un contexte de X-Ray trace.
`Span.SpanContext.TraceFlags`	Analysez l' X-Ray en-tête trouvé dans `.tracing.value` , puis utilisez la `Sampled` valeur.
`Span.Attributes`	Votre extension peut ajouter toute valeur personnalisée ici.

Cartographie des RuntimeDone événements*

OpenTelemetry	Schéma de l'API de télémétrie Lambda
`Span.Name`	Votre extension génère la valeur basée sur le champ `type`.
`Span.StartTime`	Utilisez `e.time` à partir de l'événement `*Start` correspondant. Sinon, utilisez `e.time - e.metrics.durationMs` .
`Span.EndTime`	N/A, car l'événement n'est pas encore terminé.

OpenTelemetry	Schéma de l'API de télémétrie Lambda
`Span.Kind`	Définie sur `Server`.
`Span.Status`	Si `e.status` n'est pas égal à `success`, mettez `Error`. Sinon, définissez sur `Ok`.
`Span.Events[]`	Utilisez `e.spans[]` .
`Span.Events[i].Name`	Utilisez `e.spans[i].name` .
`Span.Events[i].Time`	Utilisez `e.spans[i].start` .
`Span.TraceId`	Analysez l' AWS X-Ray en-tête trouvé dans`e.tracing.value` , puis utilisez la `TraceId` valeur.
`Span.ParentId`	Analysez l' X-Ray en-tête trouvé dans`e.tracing.value` , puis utilisez la `Parent` valeur.
`Span.SpanId`	Utilisez le même `SpanId` de l'événement `*Start`. S'il n'est pas disponible, utilisez alors `e.tracing.spanId` , ou générez un nouveau `SpanId`.
`Span.SpanContext.TraceState`	N/A pour un contexte de X-Ray trace.
`Span.SpanContext.TraceFlags`	Analysez l' X-Ray en-tête trouvé dans`e.tracing.value` , puis utilisez la `Sampled` valeur.
`Span.Attributes`	Votre extension peut ajouter toute valeur personnalisée ici.

Mappage des événements *Report

OpenTelemetry	Schéma de l'API de télémétrie Lambda
`Span.Name`	Votre extension génère la valeur basée sur le champ `type`.
`Span.StartTime`	Utilisez `e.time` à partir de l'événement `*Start` correspondant. Sinon, utilisez `e.time - e.metrics.durationMs` .
`Span.EndTime`	Utilisez `e.time`.
`Span.Kind`	Définie sur `Server`.
`Span.Status`	Utilisez la même valeur que l'événement `*RuntimeDone` .
`Span.TraceId`	Analysez l' AWS X-Ray en-tête trouvé dans`e.tracing.value` , puis utilisez la `TraceId` valeur.
`Span.ParentId`	Analysez l' X-Ray en-tête trouvé dans`e.tracing.value` , puis utilisez la `Parent` valeur.
`Span.SpanId`	Utilisez le même `SpanId` de l'événement `*Start`. S'il n'est pas disponible, utilisez alors `e.tracing.spanId` , ou générez un nouveau `SpanId`.
`Span.SpanContext.TraceState`	N/A pour un contexte de X-Ray trace.
`Span.SpanContext.TraceFlags`	Analysez l' X-Ray en-tête trouvé dans`e.tracing.value` , puis utilisez la `Sampled` valeur.
`Span.Attributes`	Votre extension peut ajouter toute valeur personnalisée ici.

Mappage vers des OTel Spans avec des Spans enfants

Le tableau suivant décrit comment convertir les événements de l'API de télémétrie Lambda en OTel Spans avec des Spans enfants (imbriqués) pour les Spans `*RuntimeDone`. Pour les mappages `*Start` et `*Report`, reportez-vous aux tableaux de the section called "Mappage vers les OTel Spans avec les événements Span", car ils sont les mêmes pour les Spans enfant. Dans cette table, e représente l'événement provenant de la source de télémétrie.

Cartographie des RuntimeDone événements*

OpenTelemetry	Schéma de l'API de télémétrie Lambda
`Span.Name`	Votre extension génère la valeur basée sur le champ `type`.
`Span.StartTime`	Utilisez `e.time` à partir de l'événement `*Start` correspondant. Sinon, utilisez `e.time - e.metrics.durationMs` .
`Span.EndTime`	N/A, car l'événement n'est pas encore terminé.
`Span.Kind`	Définie sur `Server`.
`Span.Status`	Si `e.status` n'est pas égal à `success`, mettez `Error`. Sinon, définissez sur `Ok`.
`Span.TraceId`	Analysez l' AWS X-Ray en-tête trouvé dans`e.tracing.value` , puis utilisez la `TraceId` valeur.
`Span.ParentId`	Analysez l' X-Ray en-tête trouvé dans`e.tracing.value` , puis utilisez la `Parent` valeur.
`Span.SpanId`	Utilisez le même `SpanId` de l'événement `*Start`. S'il n'est pas disponible, utilisez

OpenTelemetry	Schéma de l'API de télémétrie Lambda
	alors `e.tracing.spanId` , ou générez un nouveau `SpanId`.
`Span.SpanContext.TraceState`	N/A pour un contexte de X-Ray trace.
`Span.SpanContext.TraceFlags`	Analysez l' X-Ray en-tête trouvé dans`e.tracing.value` , puis utilisez la `Sampled` valeur.
`Span.Attributes`	Votre extension peut ajouter toute valeur personnalisée ici.
`ChildSpan[i].Name`	Utilisez `e.spans[i].name` .
`ChildSpan[i].StartTime`	Utilisez `e.spans[i].start` .
`ChildSpan[i].EndTime`	Utilisez `e.spans[i].start + e.spans[i].durations` .
`ChildSpan[i].Kind`	Identique au parent `Span.Kind` .
`ChildSpan[i].Status`	Identique au parent `Span.Status` .
`ChildSpan[i].TraceId`	Identique au parent `Span.TraceId` .
`ChildSpan[i].ParentId`	Utilisez le parent `Span.SpanId` .
`ChildSpan[i].SpanId`	Générer un nouveau `SpanId`.
`ChildSpan[i].SpanContext.TraceState`	N/A pour un contexte de X-Ray trace.
`ChildSpan[i].SpanContext.TraceFlags`	Identique au parent `Span.SpanContext.TraceFlags` .

Utilisation de l’API Logs Lambda

Important

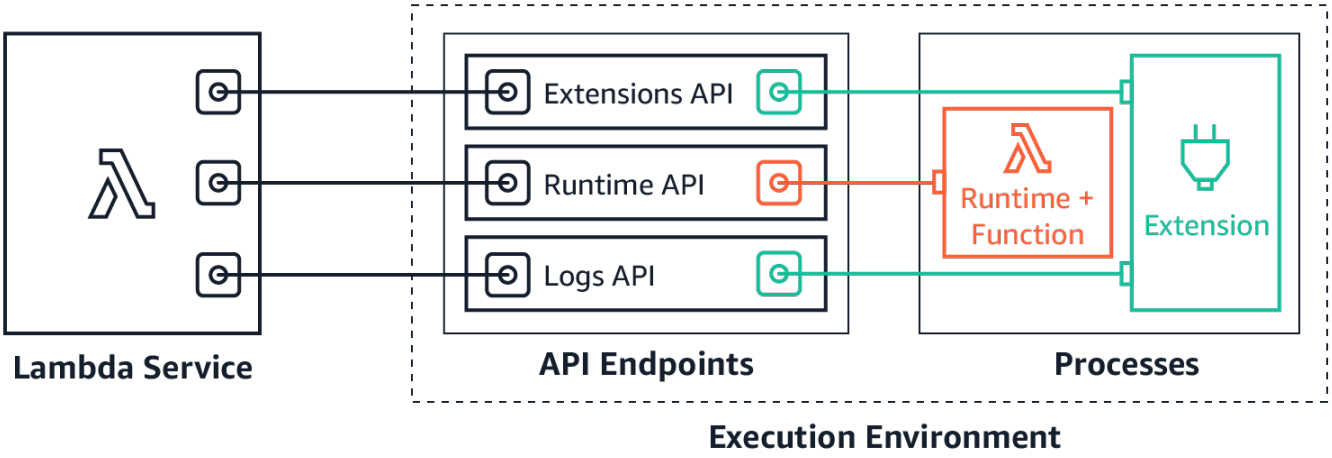
L’API de télémétrie Lambda remplace l’API de journaux Lambda. Bien que l’API de journaux reste entièrement fonctionnelle, nous vous recommandons d’utiliser uniquement l’API de télémétrie à l’avenir. Vous pouvez abonner votre extension à un flux de télémétrie en utilisant l’API de télémétrie ou l’API de journaux. Après s’être abonné à l’aide de l’une de ces API, toute tentative d’abonnement à l’aide de l’autre API renvoie une erreur.

Les instances gérées Lambda ne prennent pas en charge l'API Logs

Les instances gérées Lambda ne prennent pas en charge l'API Logs. Si vous utilisez des fonctions d'instance gérées, utilisez plutôt l'API de télémétrie. L'API de télémétrie fournit des fonctionnalités améliorées pour collecter et traiter les données de télémétrie à partir de vos fonctions d'événements Lambda.

Lambda capture automatiquement les journaux d'exécution et les diffuse vers Amazon. CloudWatch Ce flux de journal contient les journaux générés par votre code de fonction d'événement et vos extensions, ainsi que les journaux générés par Lambda dans le cadre de l'invocation de la fonction d'événement.

Les extensions Lambda peuvent utiliser l’API Lambda Runtime Logs pour s’abonner à des flux de journaux directement à partir de l’environnement d’exécution Lambda. Lambda diffuse les journaux vers l’extension qui peut ensuite les traiter, les filtrer et les envoyer à n’importe quelle destination de prédilection.



L'API Logs permet aux extensions de s'abonner à trois flux de journaux différents :

- La fonction enregistre que la fonction d'événement Lambda génère et écrit dans ou. `stdout` `stderr`
- Journaux d'extension que le code d'extension génère.
- Journaux de plateforme Lambda qui enregistrent les événements et les erreurs liés aux appels et aux extensions.

> **Note**
>
> Lambda envoie tous les journaux à CloudWatch, même lorsqu'une extension s'abonne à un ou plusieurs flux de journaux.

Rubriques

- S'abonner pour recevoir des journaux
- Utilisation de la mémoire
- Protocoles de destination
- Configuration de mise en mémoire tampon
- Exemple d'abonnement
- Exemple de code pour l'API Logs
- Référence d'API Logs

- Messages de journaux

S’abonner pour recevoir des journaux

Une extension Lambda peut s’abonner aux journaux en envoyant une demande d’abonnement à l’API Logs.

Pour vous abonner afin de recevoir des journaux, vous avez besoin de l’identifiant d’extension (`Lambda-Extension-Identifier`). Enregistrez d’abord l’extension pour recevoir l’identifiant de l’extension. Abonnez-vous ensuite à l’API Logs lors de l’initialisation. Une fois la phase d’initialisation terminée, Lambda ne traite pas les demandes d’abonnement.

> **Note**
>
> L’abonnement à l’API Logs est idempotent. Les demandes d’abonnement en double n’entraînent pas de doublons d’abonnements.

Utilisation de la mémoire

L’utilisation de la mémoire augmente de façon linéaire à mesure que le nombre d’abonnés augmente. Les abonnements consomment des ressources de mémoire car chaque abonnement ouvre un nouveau tampon mémoire pour stocker les journaux. Pour optimiser l’utilisation de la mémoire tampon, vous pouvez ajuster la configuration de la mise en mémoire tampon. L’utilisation de la mémoire tampon compte pour la consommation globale de mémoire dans l’environnement d’exécution.

Protocoles de destination

Vous pouvez choisir l’un des protocoles suivants pour recevoir les journaux :

1. HTTP (recommandé) – Lambda envoie les journaux à un point de terminaison HTTP local (`http://sandbox.localdomain:${PORT}/${PATH}`) sous la forme d’un tableau d’enregistrements au format JSON. Le paramètre `$PATH` est facultatif. Notez que seul HTTP est pris en charge, pas HTTPS. Vous pouvez choisir de recevoir des journaux via PUT ou POST.
2. TCP – Lambda envoie les journaux à un port TCP au format NDJSON (Newline delimited JSON).

Nous vous recommandons d'utiliser HTTP plutôt que TCP. Avec TCP, la plateforme Lambda ne peut pas confirmer la livraison des journaux à la couche d'application. Vous risquez par conséquent de perdre des journaux si votre extension se bloque. HTTP ne partage pas cette limitation.

Nous vous recommandons également de configurer l'écouteur HTTP local ou le port TCP avant de vous abonner pour recevoir les journaux. Au cours de l'installation, notez ce qui suit :

- Lambda n'envoie de journaux qu'à des destinations au sein de l'environnement d'exécution.
- Lambda réessaie d'envoyer les journaux (avec une interruption) s'il n'y a pas d'écouteur, ou si la requête POST ou PUT génère une erreur. Si l'abonné aux journaux se bloque, il continue de recevoir des journaux après que Lambda a redémarré l'environnement d'exécution.
- Lambda réserve le port 9001. Il n'y a pas d'autres restrictions ou recommandations relatives au numéro de port.

Configuration de mise en mémoire tampon

Lambda peut mettre les journaux en mémoire tampon avant de les livrer à l'abonné. Vous pouvez configurer ce comportement dans la demande d'abonnement en spécifiant les champs facultatifs suivants. Notez que Lambda utilise la valeur par défaut pour tout champ que vous ne spécifiez pas.

- timeoutMs – Durée maximum (en millisecondes) de mise en mémoire tampon d'un lot. Par défaut : 1 000. Minimum : 25. Maximum : 30 000.
- maxBytes – Taille maximum (en octets) des journaux à mettre en mémoire tampon. Par défaut : 262 144. Minimum : 262 144. Maximum : 1 048 576.
- maxItems – Nombre maximum d'événements à mettre en mémoire tampon. Par défaut : 10 000. Minimum : 1 000. Maximum : 10 000.

Lors de la configuration de la mise en mémoire tampon, notez les points suivants :

- Lambda vide les journaux en cas de fermeture de l'un des flux d'entrée, par exemple, si le runtime se bloque.
- Chaque abonné peut spécifier une configuration de mise en mémoire tampon différente dans sa demande d'abonnement.
- Tenez compte de la taille de tampon dont vous avez besoin pour lire les données. Attendez-vous à recevoir des charges utiles aussi volumineuses que `2*maxBytes+metadata`, où `maxBytes` est configuré dans la demande d'abonnement. Par exemple, Lambda ajoute les octets de métadonnées suivants à chaque enregistrement :

```
{
"time": "2020-08-20T12:31:32.123Z",
"type": "function",
"record": "Hello World"
}
```

- Si l'abonné ne peut pas traiter les journaux entrants assez rapidement, Lambda peut supprimer les journaux pour limiter l'utilisation de la mémoire. Pour indiquer le nombre d'enregistrements supprimés, Lambda envoie un journal `platform.logsDropped`. Pour plus d'informations, consultez the section called "Lambda : certains journaux de ma fonction n'apparaissent pas".

Exemple d'abonnement

L'exemple suivant montre une demande d'abonnement aux journaux de la plateforme et des fonctions.

```
PUT http://${AWS_LAMBDA_RUNTIME_API}/2020-08-15/logs HTTP/1.1
{ "schemaVersion": "2020-08-15",
  "types": [
      "platform",
      "function"
    ],
  "buffering": {
      "maxItems": 1000,
      "maxBytes": 262144,
      "timeoutMs": 100
    },
  "destination": {
    "protocol": "HTTP",
    "URI": "http://sandbox.localdomain:8080/lambda_logs"
  }
}
```

Si la demande réussit, l'abonné reçoit une réponse de succès HTTP 200.

```
HTTP/1.1 200 OK
"OK"
```

Exemple de code pour l'API Logs

Pour un exemple de code montrant comment envoyer des journaux vers une destination personnalisée, consultez la section Utilisation d' AWS Lambda extensions pour envoyer des journaux vers des destinations personnalisées sur le blog AWS Compute.

Pour des exemples de code Python et Go montrant comment développer une extension Lambda de base et s'abonner à l'API Logs, voir AWS Lambda Extensions dans le référentiel AWS Samples GitHub . Pour plus d'informations sur la génération d'une extension Lambda, consultez the section called "API d'extensions".

Référence d'API Logs

Vous pouvez extraire le point de terminaison d'API Logs à partir de la variable d'environnement `AWS_LAMBDA_RUNTIME_API`. Pour envoyer une demande d'API, utilisez le préfixe `2020-08-15/` avant le chemin d'accès de l'API. Exemples :

```
http://${AWS_LAMBDA_RUNTIME_API}/2020-08-15/logs
```

La spécification OpenAPI pour la version d'API Logs 2020-08-15 est disponible ici : logs-api-request.zip.

S'abonner

Pour s'abonner à un ou plusieurs des flux de journal disponibles dans l'environnement d'exécution Lambda, les extensions envoient une demande d'API Subscribe.

Chemin – `/logs`

Méthode – PUT

Paramètres de corps

`destination` – Voir the section called "Protocoles de destination". Obligatoire : oui. Type : chaînes.

`buffering` – Voir the section called "Configuration de mise en mémoire tampon". Requis : non. Type : chaînes.

`types` – Tableau des types de journaux à recevoir. Obligatoire : oui. Type : tableau de chaînes. Valeurs valides : « plateforme », « fonction», « extension ».

`schemaVersion` – Obligatoire : non. Valeur par défaut : « 2020-08-15 ». Attribuez la valeur « 2021-03-18 » pour que l'extension reçoive les messages `platform.runtimeDone`.

Paramètres de réponse

Les spécifications OpenAPI pour les réponses d'abonnement version 2020-08-15 sont disponibles pour les protocoles HTTP et TCP :

- HTTP : logs-api-http-response.zip
- TCP : logs-api-tcp-response.zip

Codes de réponse

- 200 – Demande effectuée avec succès.
- 202 – Demande acceptée. Réponse à une demande d'abonnement pendant les tests locaux.
- 4XX – Demande erronée.
- 500 – Erreur de service.

Si la demande réussit, l'abonné reçoit une réponse de succès HTTP 200.

```
HTTP/1.1 200 OK
"OK"
```

Si la demande échoue, l'abonné reçoit une réponse d'erreur. Exemples :

```
HTTP/1.1 400 OK
{
    "errorType": "Logs.ValidationError",
    "errorMessage": URI port is not provided; types should not be empty"
}
```

Messages de journaux

L'API Logs permet aux extensions de s'abonner à trois flux de journaux différents :

- Fonction : enregistre ce que la fonction d'événement Lambda génère et écrit dans ou. `stdout` `stderr`
- Extension – Journaux que le code d'extension génère.
- Plateforme – Journaux que la plateforme de runtime génère, qui consignent des événements et des erreurs liés aux appels et aux extensions.

Rubriques

- Journaux de fonctions
- Journaux d'extension
- Journaux de plateforme

Journaux de fonctions

La fonction d'événement Lambda et les extensions internes génèrent des journaux de fonctions et les écrivent dans ou. `stdout` `stderr`

L'exemple suivant montre le format d'un message du journal des fonctions. {« time » : « 2020-08-20 », T12:31:32.123Z « type » : « function », « record » : « ERREUR détectée. Stack trace:\n\my-function (line 10)\n" }

Journaux d'extension

Les extensions peuvent générer des journaux d'extensions. Le format du journal est le même que pour un journal de fonction.

Journaux de plateforme

Lambda génère des messages de journal pour des événements de plateforme tels que `platform.start`, `platform.end` et `platform.fault`.

Vous pouvez éventuellement vous abonner à la version 2021-03-18 du schéma de l'API Logs, qui inclut le message de journal `platform.runtimeDone`.

Exemple de messages du journal de la plateforme

L'exemple suivant montre les journaux de début et de fin de la plateforme. Ces journaux indiquent l'heure de début et de fin de l'appel pour l'appel spécifié par le requestId.

```
{
    "time": "2020-08-20T12:31:32.123Z",
    "type": "platform.start",
    "record": {"requestId": "6f7f0961f83442118a7af6fe80b88d56"}
}
{
    "time": "2020-08-20T12:31:32.123Z",
    "type": "platform.end",
```

```
    "record": {"requestId": "6f7f0961f83442118a7af6fe80b88d56"}
}
```

Le message du RuntimeDone journal platform.init indique l'état de la `Runtime init` sous-phase, qui fait partie de la phase du cycle de vie d'initialisation. Lorsque `Runtime init` est réussie, l'environnement d'exécution envoie une demande d'API d'exécution `/next` (pour les types d'initialisation `on-demand` et `provisioned-concurrency`) ou `restore/next` (pour le type d'initialisation `snap-start`). L'exemple suivant montre un message de RuntimeDone journal platform.init réussi pour le type d'initialisation. `snap-start`

```
{
  "time":"2022-07-17T18:41:57.083Z",
  "type":"platform.initRuntimeDone",
  "record":{
      "initializationType":"snap-start",
      "status":"success"
  }
}
```

Le message de journal platform.initReport indique la durée de la phase `Init` et le nombre de millisecondes qui vous ont été facturées pendant cette phase. Lorsque le type d'initialisation est `provisioned-concurrency`, Lambda envoie ce message pendant l'appel. Lorsque le type d'initialisation est `snap-start`, Lambda envoie ce message après avoir restauré l'instantané. L'exemple suivant montre un message de journal platform.initReport pour le type d'initialisation `snap-start`.

```
{
  "time":"2022-07-17T18:41:57.083Z",
  "type":"platform.initReport",
  "record":{
      "initializationType":"snap-start",
      "metrics":{
          "durationMs":731.79,
          "billedDurationMs":732
          }
  }
}
```

Le journal du rapport de la plateforme inclut des métriques relatives à l'appel spécifié par le requestId. Le champ `initDurationMs` n'est inclus dans le journal que si l'appel comprend un démarrage à

froid. Si le AWS X-Ray suivi est actif, le journal inclut des X-Ray métadonnées. L'exemple suivant montre un journal de rapport de la plateforme pour un appel qui comprend un démarrage à froid.

```
{
    "time": "2020-08-20T12:31:32.123Z",
    "type": "platform.report",
    "record": {"requestId": "6f7f0961f83442118a7af6fe80b88d56",
        "metrics": {"durationMs": 101.51,
            "billedDurationMs": 300,
            "memorySizeMB": 512,
            "maxMemoryUsedMB": 33,
            "initDurationMs": 116.67
        }
    }
}
```

Le journal des pannes de la plateforme capture les erreurs d'exécution ou d'environnement d'exécution. L'exemple suivant montre un message de journal des erreurs de plateforme.

```
{
    "time": "2020-08-20T12:31:32.123Z",
    "type": "platform.fault",
    "record": "RequestId: d783b35e-a91d-4251-af17-035953428a2c Process exited before
 completing request"
}
```

> **Note**
>
> AWS met actuellement en œuvre des modifications du service Lambda. En raison de ces modifications, vous pouvez constater des différences mineures entre la structure et le contenu des messages du journal système et des segments de trace émis par les différentes fonctions d'événement Lambda de votre ordinateur. Compte AWS
> L'une des sorties de journal concernées par cette modification est le champ `"record"` du journal des erreurs de plateforme. Les exemples suivants montrent des champs `"record"` illustratifs dans les anciens et les nouveaux formats. Le nouveau format de journal des erreurs contient un message plus concis
> Ces modifications seront mises en œuvre au cours des prochaines semaines, et toutes les fonctions, Régions AWS sauf en Chine et dans les GovCloud régions, passeront à l'utilisation du nouveau format des messages de journal et des segments de trace.

Example enregistrement du journal des erreurs de plateforme (ancien format)

```
"record":"RequestId: ...\tError: Runtime exited with error: exit status
 255\nRuntime.ExitError"
```

Example enregistrement du journal des erreurs de plateforme (nouveau format)

```
"record":"RequestId: ... Status: error\tErrorType: Runtime.ExitError"
```

Lambda génère un journal d'extension de plateforme quand une extension s'enregistre auprès de l'API d'extensions. L'exemple suivant montre un message d'extension de la plateforme.

```
{
    "time": "2020-08-20T12:31:32.123Z",
    "type": "platform.extension",
    "record": {"name": "Foo.bar",
        "state": "Ready",
        "events": ["INVOKE", "SHUTDOWN"]
     }
}
```

Lambda génère un journal d'abonnement aux journaux de plateforme quand une extension s'abonne à l'API Logs. L'exemple suivant montre un message d'abonnement aux journaux.

```
{
    "time": "2020-08-20T12:31:32.123Z",
    "type": "platform.logsSubscription",
    "record": {"name": "Foo.bar",
        "state": "Subscribed",
        "types": ["function", "platform"],
    }
}
```

Lambda génère un journal des journaux de plateforme supprimés quand une extension n'est pas en mesure de traiter le nombre de journaux qu'elle reçoit. L'exemple suivant montre un message de journal `platform.logsDropped`.

```
{
    "time": "2020-08-20T12:31:32.123Z",
```

```
    "type": "platform.logsDropped",
    "record": {"reason": "Consumer seems to have fallen behind as it has not
 acknowledged receipt of logs.",
        "droppedRecords": 123,
        "droppedBytes" 12345
    }
}
```

Le message de journal platform.restoreStart indique l'heure à laquelle la phase `Restore` a démarré (type d'initialisation `snap-start` uniquement). Exemple :

```
{
  "time":"2022-07-17T18:43:44.782Z",
  "type":"platform.restoreStart",
  "record":{}
}
```

Le message de journal platform.restoreReport indique la durée de la phase `Restore` et le nombre de millisecondes qui vous ont été facturées pendant cette phase (type d'initialisation `snap-start` uniquement). Exemple :

```
{
  "time":"2022-07-17T18:43:45.936Z",
  "type":"platform.restoreReport",
  "record":{
      "metrics":{
          "durationMs":70.87,
          "billedDurationMs":13
      }
  }
}
```

Messages **`RuntimeDone`** de la plateforme

Si vous définissez la version du schéma sur « 18/03/2021 » dans la demande d'abonnement, Lambda envoie un `platform.runtimeDone` message une fois l'appel de la fonction d'événement terminé avec succès ou avec une erreur. L'extension peut utiliser ce message pour arrêter toute collecte de télémétrie pour cet appel de fonction d'événement.

La spécification OpenAPI pour le type d'événement Log dans la version de schéma 2021-03-18 est disponible ici : schema-2021-03-18.zip

Lambda génère le message de journal `platform.runtimeDone` quand le runtime envoie une demande d'API de runtime `Next` ou `Error`. Le journal `platform.runtimeDone` informe les utilisateurs de l'API Logs que l'appel de fonction se termine. Les extensions peuvent utiliser ces informations pour décider quand envoyer toutes les données télémétriques collectées au cours de cet appel.

Exemples

Lambda envoie le message `platform.runtimeDone` après que le runtime a envoyé la demande NEXT à l'issue de l'appel de fonction. Les exemples suivants présentent des messages pour chacune des valeurs de statut : succès, échec et expiration du délai.

Example Exemple de message de réussite

```
{
    "time": "2021-02-04T20:00:05.123Z",
    "type": "platform.runtimeDone",
    "record": {
       "requestId":"6f7f0961f83442118a7af6fe80b88",
       "status": "success"
    }
}
```

Example Exemple de message d'échec

```
{
   "time": "2021-02-04T20:00:05.123Z",
   "type": "platform.runtimeDone",
   "record": {
      "requestId":"6f7f0961f83442118a7af6fe80b88",
      "status": "failure"
   }
}
```

Example Exemple de message d'expiration du délai

```
{
   "time": "2021-02-04T20:00:05.123Z",
   "type": "platform.runtimeDone",
   "record": {
      "requestId":"6f7f0961f83442118a7af6fe80b88",
      "status": "timeout"
```

```
  }
}
```

Example Exemple de RuntimeDone message platform.restore (type d'initialisation **`snap-start uniquement`**)

Le message du RuntimeDone journal platform.restore indique si la `Restore` phase a réussi ou non. Lambda envoie ce message lorsque l'environnement d'exécution envoie une demande d'API d'exécution `restore/next`. Il existe trois statuts possibles : succès, échec et dépassement de délai. L'exemple suivant montre un message du journal platform.restore RuntimeDone réussi.

```
{
  "time":"2022-07-17T18:43:45.936Z",
  "type":"platform.restoreRuntimeDone",
  "record":{
      "status":"success"
  }
}
```

Résolution des problèmes dans Lambda

Les rubriques suivantes fournissent des conseils de dépannage pour les erreurs et les problèmes que vous pouvez rencontrer lors de l'utilisation de l'API, de la console ou des outils Lambda. Si vous rencontrez un problème qui n'est pas répertorié ici, vous pouvez utiliser le bouton Commentaire sur cette page pour le signaler.

Pour plus de conseils de dépannage et de réponses aux questions courantes de support, visitez le Centre de connaissances AWS.

Pour plus d'informations sur le débogage et le dépannage des applications Lambda, consultez Débogage dans Serverless Land.

Rubriques

- Résoudre les problèmes de configuration dans Lambda
- Résoudre les problèmes de déploiement dans Lambda
- Résoudre les problèmes d'invocation dans Lambda
- Résoudre les problèmes d'exécution dans Lambda
- Résoudre les problèmes de mappage des sources d'événements dans Lambda

- Résolution des problèmes de réseaux dans Lambda

Résoudre les problèmes de configuration dans Lambda

Les paramètres de configuration de votre fonction peuvent avoir un impact sur les performances globales et le comportement de votre fonction d'événement Lambda. Elles peuvent ne pas provoquer d'erreurs de fonctionnement réelles, mais peuvent entraîner des délais et des résultats inattendus.

Les rubriques suivantes fournissent des conseils de dépannage pour les problèmes courants que vous pourriez rencontrer avec les paramètres de configuration des fonctions Lambda.

Rubriques

- Configurations de mémoire
- CPU-bound configurations
- Délais
- Fuite de mémoire entre les invocations
- Résultats asynchrones renvoyés à une invocation ultérieure

Configurations de mémoire

Vous pouvez configurer une fonction Lambda à utiliser entre 128 Mo et 10 240 Mo de mémoire. Par défaut, la plus petite quantité de mémoire est affectée à toutes les fonctions créées dans la console. De nombreuses fonctions Lambda sont performantes à ce réglage le plus bas. Toutefois, si vous importez de grandes bibliothèques de code ou si vous effectuez des tâches gourmandes en mémoire 128 Mo ne suffisent pas.

Si vos fonctions s’exécutent beaucoup plus lentement que prévu, la première étape consiste à augmenter le paramètre de mémoire. Pour les fonctions liées à la mémoire, cela permet de résoudre le problème et d'améliorer les performances de votre fonction.

CPU-bound configurations

Pour les opérations gourmandes en ressources informatiques, si les performances de votre fonction sont plus lentes que prévu, cela peut être dû au fait que votre fonction est. CPU-bound Dans ce cas, la capacité de calcul de la fonction ne peut pas suivre le rythme de la tâche.

Lambda ne vous permet pas de modifier directement la configuration du processeur, mais le processeur est contrôlé indirectement par le biais des paramètres de mémoire. Le service Lambda

alloue proportionnellement plus de processeur virtuel à mesure que vous allouez de la mémoire. Avec 1,8 Go de mémoire, un processeur virtuel entier est alloué à une fonction Lambda et, au-dessus de ce niveau, elle a accès à plusieurs cœurs de processeurs virtuels. Avec 10 240 Mo, elle dispose de six processeurs virtuels disponibles. En d'autres termes, vous pouvez améliorer les performances en augmentant l'allocation de mémoire, même si la fonction n'utilise pas toute la mémoire.

Délais

Les délais d’expiration des fonctions Lambda peuvent être définis entre 1 et 900 secondes (15 minutes). Pour les fonctions utilisant des instances AWS Lambda gérées, les invocations asynchrones et les invocations de mappage des sources d'événements (sauf Amazon MQ et Amazon DocumentDB) prennent en charge une valeur maximale autorisée de 5 400 secondes (90 minutes). Par défaut, la console Lambda définit ce paramètre sur 3 secondes. La valeur du délai d’expiration est une soupape de sécurité qui garantit que les fonctions ne s’exécutent pas indéfiniment. Une fois le délai d’expiration atteint, Lambda arrête l’invocation de fonction.

Si une valeur de délai d'expiration est définie à une valeur proche de la durée moyenne d'une fonction, cela augmente le risque que la fonction expire de façon inattendue. La durée d’une fonction peut varier en fonction de la quantité de données transférées et traitées, ainsi que de la latence des services avec lesquels la fonction interagit. Les causes courantes de délai d’expiration comprennent les suivantes :

- Lorsque vous téléchargez des données depuis des compartiments S3 ou d’autres entrepôts de données, le téléchargement est plus important ou prend plus de temps que la moyenne.
- Une fonction envoie une requête à un autre service, qui met plus de temps à répondre.
- Les paramètres fournis à une fonction nécessitent une complexité de calcul accrue dans la fonction, ce qui fait que l’invocation prend plus de temps.

Lors des tests de votre application, veillez à ce que ceux-ci reflètent fidèlement la taille et la quantité des données, et à ce que les valeurs des paramètres soient réalistes. Il est important d’utiliser des jeux de données se situant dans les limites supérieures de ce que l’on peut raisonnablement attendre de votre charge de travail.

En outre, implémentez des limites supérieures à votre charge de travail dans la mesure du possible. Dans cet exemple, l’application peut utiliser une limite de taille maximale pour chaque type de fichier. Vous pouvez ensuite tester les performances de votre application pour une gamme de tailles de fichiers attendues, jusqu’aux limites maximales incluses.

Fuite de mémoire entre les invocations

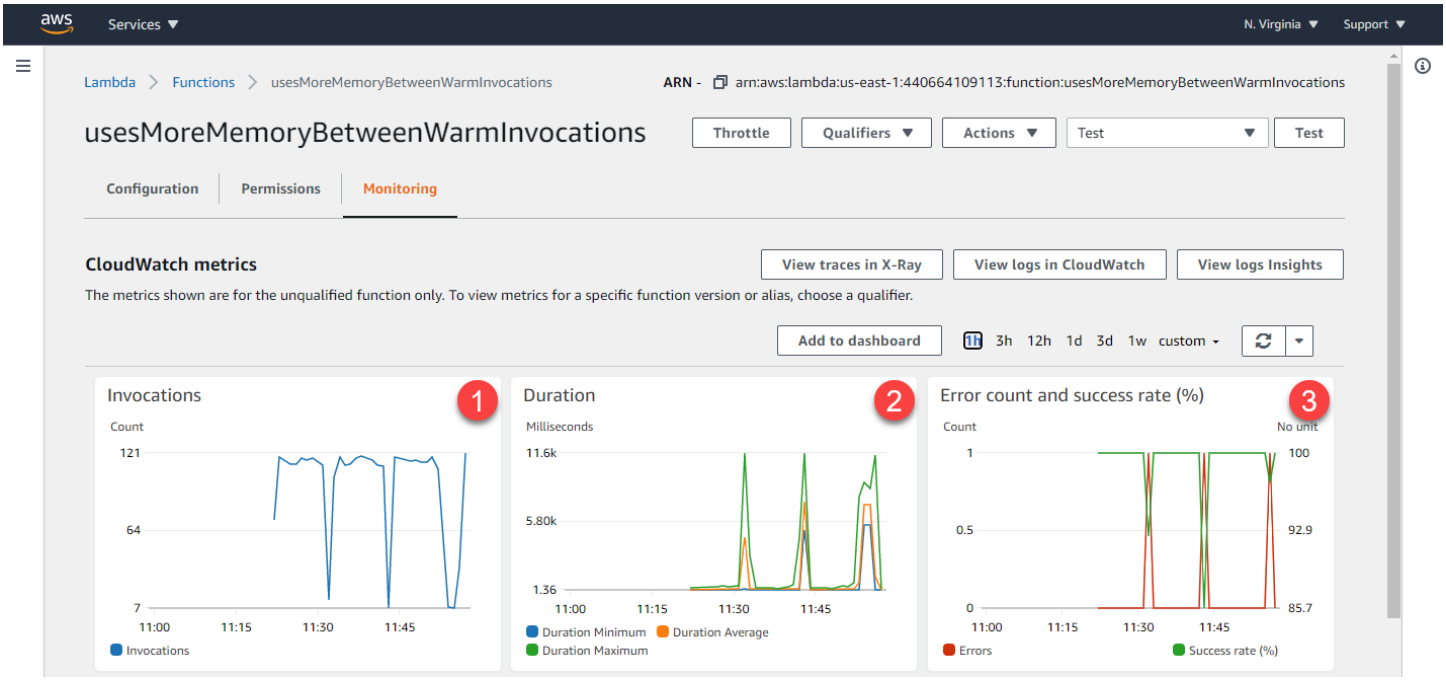
Les variables globales et les objets stockés dans la phase INIT d'une invocation Lambda conservent leur état entre les invocations à chaud. Ils ne sont complètement réinitialisés que lorsque l'environnement d'exécution est exécuté pour la première fois (également appelé « démarrage à froid »). Toutes les variables stockées dans le gestionnaire sont détruites lorsque le gestionnaire se ferme. Il est recommandé d'utiliser la phase INIT pour configurer les connexions aux bases de données, charger des bibliothèques, créer des caches et charger des actifs immuables.

Lorsque vous utilisez des bibliothèques tierces pour plusieurs invocations dans le même environnement d'exécution, consultez leur documentation pour en savoir plus sur leur utilisation dans un environnement de calcul sans serveur. Certaines bibliothèques de connexion à la base de données et de journalisation peuvent enregistrer des résultats d'appel intermédiaires et d'autres données. Cela entraîne une augmentation de l'utilisation de la mémoire de ces bibliothèques lors des invocations à chaud ultérieures. Dans ce cas, il se peut que la fonction Lambda manque de mémoire, même si votre code personnalisé élimine correctement les variables.

Ce problème affecte les invocations survenant dans des environnements d'exécution à chaud. Par exemple, le code suivant crée une fuite de mémoire entre les invocations. La fonction Lambda consomme de la mémoire supplémentaire à chaque invocation en augmentant la taille d'un tableau global :

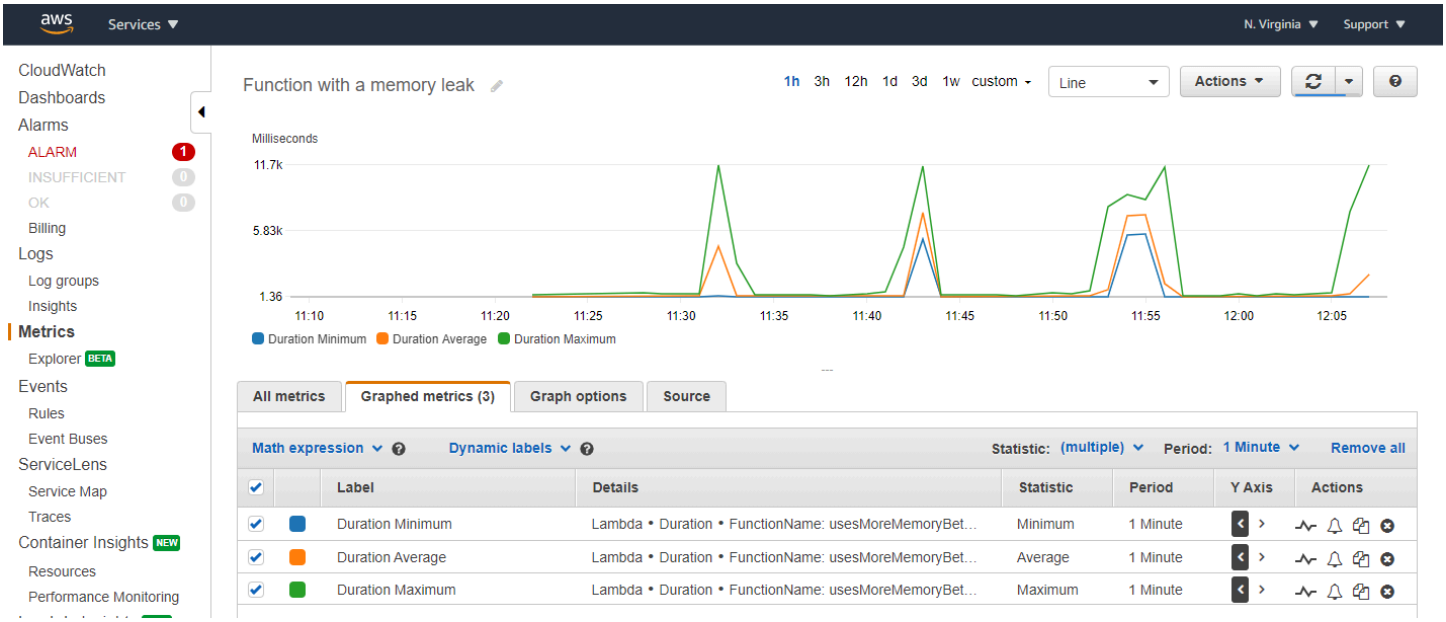
```
let a = []

exports.handler = async (event) => {
    a.push(Array(100000).fill(1))
}
```

Configuré avec 128 Mo de mémoire, après avoir invoqué cette fonction 1 000 fois, l'onglet Surveillance de la fonction Lambda affiche les modifications typiques des invocations, de la durée et du nombre d'erreurs en cas de fuite de mémoire :



1. Invocations : un taux de transaction stable est interrompu périodiquement, car les invocations prennent plus de temps à être effectuées. En régime permanent, la fuite de mémoire ne consomme pas toute la mémoire allouée à la fonction. À mesure que les performances se dégradent, le système d'exploitation appelle le stockage local pour s'adapter à l'augmentation de la mémoire requise par la fonction, ce qui réduit le nombre de transactions effectuées.
2. Durée : avant que la fonction ne soit à court de mémoire, elle termine les invocations au rythme constant d'un nombre de millisecondes à deux chiffres. Au fur et à mesure que les appels se produisent, la durée s'allonge d'un ordre de grandeur.
3. Nombre d'erreurs : lorsque la fuite de mémoire dépasse la mémoire allouée, les erreurs de fonction finissent par se produire en raison du dépassement du délai d'expiration par le calcul, ou l'environnement d'exécution arrête la fonction.

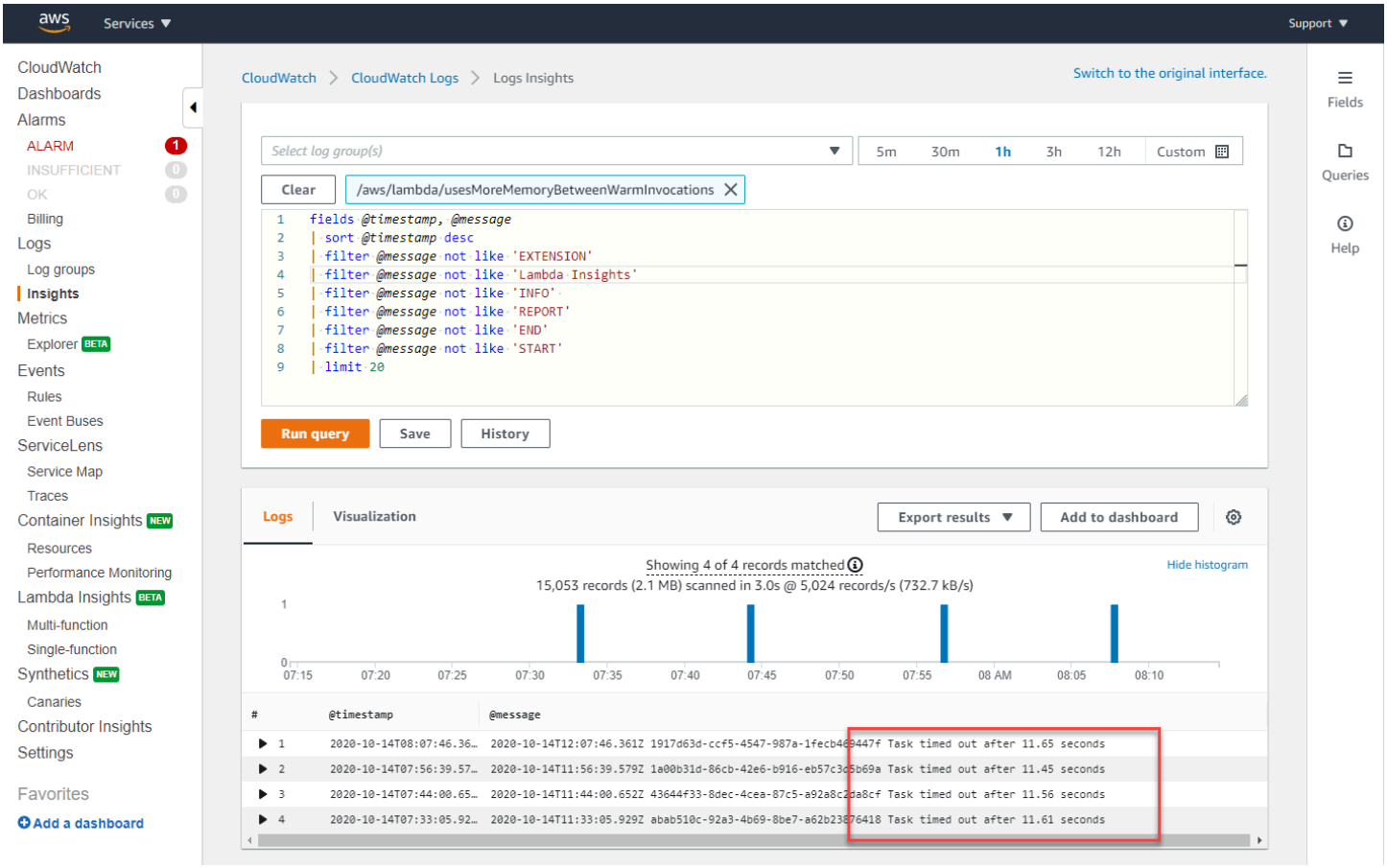
Après l'erreur, Lambda redémarre l'environnement d'exécution, ce qui explique pourquoi on observe un retour à l'état d'origine dans les trois graphiques. L'extension CloudWatch des métriques relatives à la durée fournit des informations plus détaillées sur les statistiques relatives à la durée minimale, maximale et moyenne :



Pour identifier les erreurs générées lors des 1000 appels, vous pouvez utiliser le langage de requête CloudWatch Insights. La requête suivante exclut les journaux d'information pour signaler uniquement les erreurs :

```
fields @timestamp, @message
| sort @timestamp desc
| filter @message not like 'EXTENSION'
| filter @message not like 'Lambda Insights'
| filter @message not like 'INFO'
| filter @message not like 'REPORT'
| filter @message not like 'END'
| filter @message not like 'START'
```

Lorsqu'elle est exécutée sur le groupe de journaux pour cette fonction, cela montre que les délais d'expiration sont à l'origine des erreurs périodiques :



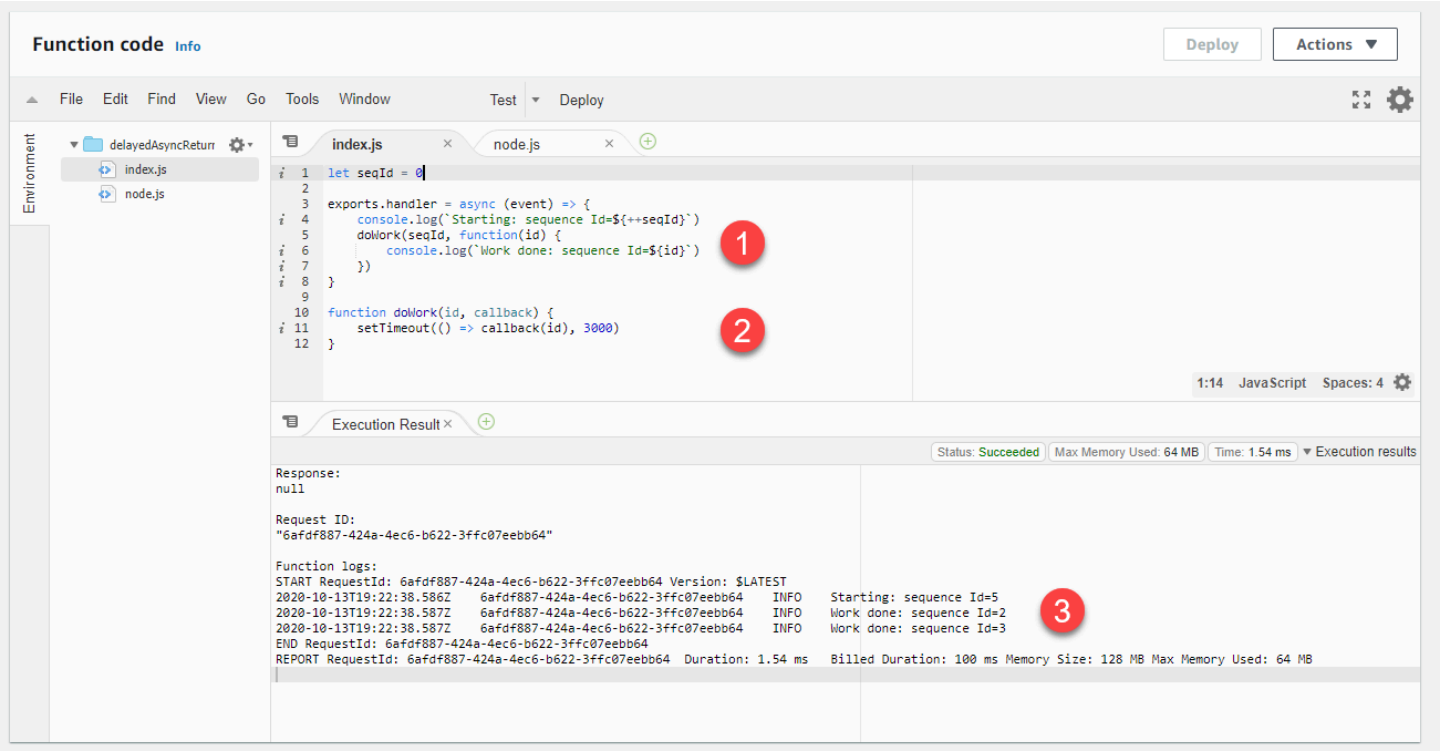
Résultats asynchrones renvoyés à une invocation ultérieure

Pour le code de fonction qui utilise des modèles asynchrones, il est possible que les résultats du rappel d'un appel soient renvoyés lors d'un futur appel. Cet exemple utilise Node.js, mais la même logique peut s'appliquer à d'autres environnements d'exécution utilisant des modèles asynchrones. La fonction utilise la syntaxe de rappel traditionnelle dans JavaScript. Elle appelle une fonction asynchrone avec un compteur incrémentiel qui suit le nombre d'invocations :

```
let seqId = 0

exports.handler = async (event, context) => {
    console.log(`Starting: sequence Id=${++seqId}`)
    doWork(seqId, function(id) {
        console.log(`Work done: sequence Id=${id}`)
    })
}

function doWork(id, callback) {
    setTimeout(() => callback(id), 3000)
```

```
}
```

Lorsqu'ils sont invoqués plusieurs fois de suite, les résultats des rappels apparaissent lors des invocations suivantes :



1. Le code appelle la fonction `doWork` en fournissant une fonction de rappel comme dernier paramètre.
2. La fonction `doWork` met un certain temps à s'exécuter avant d'invoquer le rappel.
3. La journalisation de la fonction indique que l'invocation prend fin avant la fin de l'exécution de la `doWork` fonction. De plus, après le démarrage d'une itération, les rappels des itérations précédentes sont traités, comme indiqué dans les journaux.

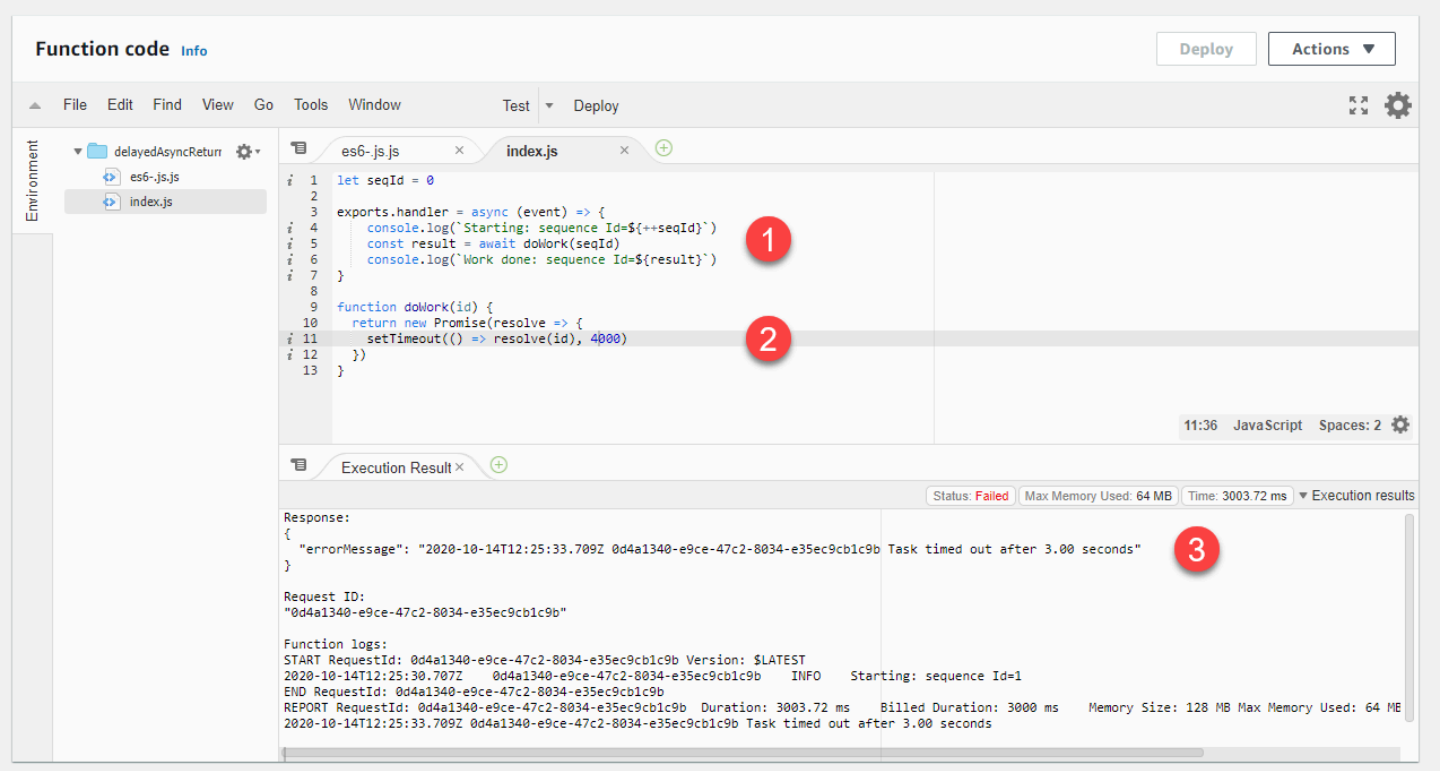
Dans JavaScript, les rappels asynchrones sont gérés par une boucle d'événements. D'autres environnements d'exécution utilisent des mécanismes différents pour gérer la simultanéité. Lorsque l'environnement d'exécution de la fonction prend fin, Lambda bloque l'environnement jusqu'au prochain appel.

Après sa reprise, JavaScript poursuit le traitement de la boucle d'événements, qui inclut dans ce cas un rappel asynchrone issu d'un appel précédent. Sans ce contexte, il peut sembler que la fonction exécute du code sans raison et renvoie des données arbitraires. En réalité, il s'agit vraiment d'un artefact de la façon dont la simultanéité d'exécution et les environnements d'exécution interagissent.

Cela crée le risque que les données privées d'une précédente invocation apparaissent lors d'une invocation ultérieure. Il existe deux façons d'empêcher ou de détecter ce comportement. Tout d'abord, JavaScript fournit les mots clés async et wait pour simplifier le développement asynchrone et également forcer l'exécution du code à attendre la fin d'un appel asynchrone. La fonction ci-dessus peut être réécrite en utilisant cette approche comme suit :

```
let seqId = 0
exports.handler = async (event) => {
    console.log(`Starting: sequence Id=${++seqId}`)
    const result = await doWork(seqId)
    console.log(`Work done: sequence Id=${result}`)
}

function doWork(id) {
  return new Promise(resolve => {
    setTimeout(() => resolve(id), 4000)
  })
}
```

L'utilisation de cette syntaxe empêche le gestionnaire de se fermer avant la fin de la fonction asynchrone. Dans ce cas, si le rappel prend plus de temps que le délai d'expiration de la fonction Lambda, la fonction renvoie une erreur au lieu de renvoyer le résultat du rappel lors d'un appel ultérieur :

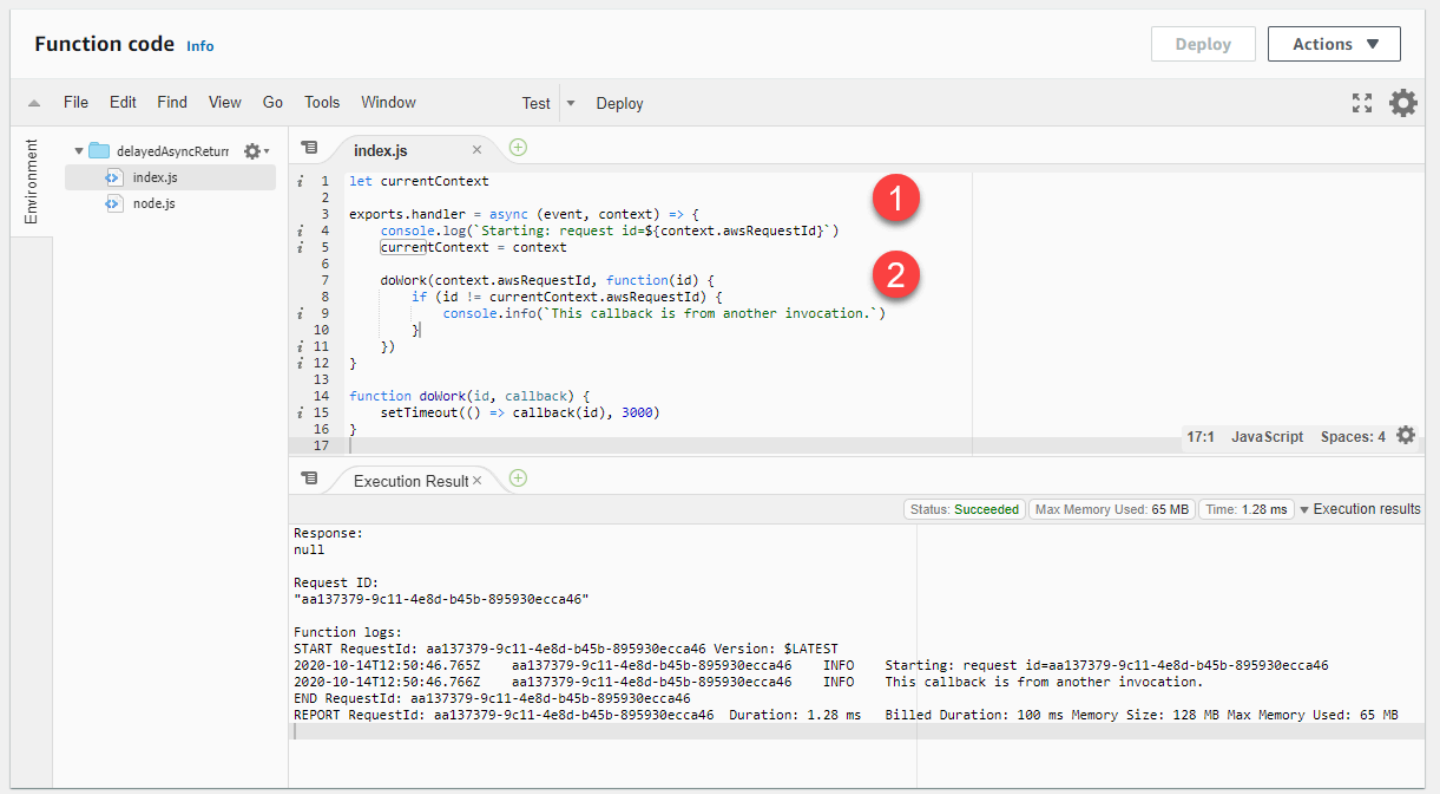


1. Le code appelle la fonction asynchrone `doWork` à l'aide du mot clé await dans le gestionnaire.
2. La fonction `doWork` met un certain temps à s'exécuter avant de résoudre la promesse.
3. La fonction expire, car `doWork` prend plus de temps que le délai imparti et le résultat du rappel n'est pas renvoyé lors d'une invocation ultérieure.

En général, assurez-vous que les processus d'arrière-plan ou les rappels dans le code se terminent avant que l'exécution du code ne prenne fin. Si cela n'est pas possible dans votre cas d'utilisation, vous pouvez utiliser un identifiant pour vous assurer que le rappel appartient à l'invocation en cours. Pour ce faire, vous pouvez utiliser les aws RequestId fournis par l'objet de contexte. En transmettant cette valeur au rappel asynchrone, vous pouvez comparer la valeur transmise à la valeur actuelle pour détecter si le rappel provient d'une autre invocation :

```
let currentContext

exports.handler = async (event, context) => {
    console.log(`Starting: request id=$\{context.awsRequestId}`)
    currentContext = context

    doWork(context.awsRequestId, function(id) {
        if (id != currentContext.awsRequestId) {
```

```
            console.info(`This callback is from another invocation.`)
        }
    })

}

function doWork(id, callback) {
    setTimeout(() => callback(id), 3000)

}
```



1. Le gestionnaire de fonctions Lambda utilise le paramètre context, qui donne accès à un ID de requête d'invocation unique.
2. L'`awsRequestId` est transmis à la fonction doWork. Dans le rappel, l'ID est comparé à la valeur `awsRequestId` de l'invocation en cours. Si ces valeurs sont différentes, le code peut agir en conséquence.

Résoudre les problèmes de déploiement dans Lambda

Lorsque vous mettez à jour votre fonction d'événement Lambda, Lambda déploie la modification en lançant de nouvelles instances de la fonction avec le code ou les paramètres mis à jour. Les erreurs de déploiement empêchent l'utilisation de la nouvelle version et peuvent résulter de problèmes liés au package de déploiement, au code, à vos autorisations ou à vos outils.

Lorsque vous déployez des mises à jour de votre fonction directement avec l'API Lambda ou avec un client tel que le AWS CLI, vous pouvez voir les erreurs provenant de Lambda directement dans la sortie. Si vous utilisez des services tels que AWS CloudFormation AWS CodeDeploy, ou AWS CodePipeline, recherchez la réponse de Lambda dans les journaux ou le flux d'événements de ce service.

Les rubriques suivantes fournissent des conseils de dépannage pour les erreurs et les problèmes que vous pouvez rencontrer lors de l'utilisation de l'API, de la console ou des outils Lambda. Si vous rencontrez un problème qui n'est pas répertorié ici, vous pouvez utiliser le bouton Commentaire sur cette page pour le signaler.

Pour plus de conseils de dépannage et de réponses aux questions courantes de support, visitez le Centre de connaissances AWS.

Pour plus d'informations sur le débogage et le dépannage des applications Lambda, consultez Débogage dans Serverless Land.

Rubriques

- Général : L'autorisation est refusée ou Impossible de charger ce fichier
- Général : Une erreur se produit lors de l'appel du UpdateFunctionCode
- Amazon S3 : code d'erreur PermanentRedirect.
- Général : impossible de trouver, impossible de charger, impossible d'importer, classe introuvable, aucun fichier ou répertoire de ce type
- Général : gestionnaire de méthode non défini
- Général : limite de stockage du code Lambda dépassée
- Lambda : échec de la conversion de couche
- Lambda : ou InvalidParameterValueException RequestEntityTooLargeException
- Lambda : InvalidParameterValueException
- Lambda : quotas de simultanéité et de mémoire

- Lambda : configuration d'alias non valide pour la simultanéité provisionnée.

Général : L'autorisation est refusée ou Impossible de charger ce fichier

Erreur : EACCES : autorisation refusée, ouvrez '/ var/task /index.js '

Erreur : impossible de charger ce fichier - cette fonction

Erreur : [Errno 13] Autorisation refusée : '/ var/task /function.py '

Le runtime Lambda a besoin d'une autorisation pour lire les fichiers de votre package de déploiement. Dans la notation octale des autorisations Linux, Lambda a besoin de 644 autorisations pour les fichiers non exécutables (rw-r--r--) et de 755 autorisations (rwxr-xr-x) pour les répertoires et les fichiers exécutables.

Sous Linux et macOS, utilisez la commande `chmod` pour modifier les autorisations de fichiers sur les fichiers et les répertoires de votre package de déploiement. Par exemple, pour octroyer à un fichier non exécutable les autorisations correctes, exécutez la commande suivante.

```
chmod 644 <filepath>
```

Pour modifier les autorisations relatives aux fichiers dans Windows, voir Définir, afficher, modifier ou supprimer des autorisations sur un objet dans la documentation Microsoft Windows.

> **Note**
>
> Si vous n'octroyez pas à Lambda les autorisations dont il a besoin pour accéder aux répertoires de votre package de déploiement, Lambda définit les autorisations de ces répertoires à 755 (rwxr-xr-x).

Général : Une erreur se produit lors de l'appel du UpdateFunctionCode

Erreur : une erreur s'est produite (RequestEntityTooLargeException) lors de l'appel de l' UpdateFunctionCode opération

Lorsque vous chargez un package de déploiement ou une archive de couche directement dans Lambda, la taille du fichier ZIP est limitée à 50 Mo. Pour charger un fichier plus volumineux, stockez-le dans Amazon S3, puis utilisez les paramètres S3Bucket et S3Key.

> **Note**
>
> Lorsque vous téléchargez un fichier directement avec le AWS CLI AWS SDK ou autre, le fichier ZIP binaire est converti en base64, ce qui augmente sa taille d'environ 30 %. Pour permettre cela et aussi prendre en compte la taille d'autres paramètres dans la demande, la limite de taille réelle de demande que Lambda applique est supérieure. Pour cette raison, la limite de 50 Mo est approximative.

Amazon S3 : code d'erreur PermanentRedirect.

Erreur : une erreur s'est produite pendant GetObject. Code d'erreur S3 : PermanentRedirect. Message d'erreur S3 : Le compartiment se trouve dans cette région : us-east-2. Veuillez utiliser cette région pour renouveler la demande

Lorsque vous chargez le package de déploiement d'une fonction à partir d'un compartiment Amazon S3, le compartiment doit se trouver dans la même région que la fonction. Ce problème peut se produire lorsque vous spécifiez un objet Amazon S3 dans un appel à UpdateFunctionCode, ou lorsque vous utilisez les commandes de package et de déploiement dans l'interface de ligne de AWS SAM commande AWS CLI ou CLI. Créez un compartiment d'artefact de déploiement pour chaque région dans laquelle vous développez des applications.

Général : impossible de trouver, impossible de charger, impossible d'importer, classe introuvable, aucun fichier ou répertoire de ce type

Erreur : module 'function' introuvable

Erreur : impossible de charger ce fichier - cette fonction

Erreur : impossible d'importer le module 'function'

Erreur : Classe introuvable : Function.handler

Erreur : fork/exec /var/task/function : aucun fichier ou répertoire de ce type

Erreur : Impossible de charger le type « Function.Handler » à partir de l'assemblage « Fonction ».

Le nom du fichier ou de la classe dans la configuration du gestionnaire de votre fonction ne correspond pas à votre code. Consultez la section suivante pour plus d'informations.

Général : gestionnaire de méthode non défini

Erreur : index.handler n'est pas défini ou n'est pas exporté

Erreur : gestionnaire 'handler' manquant dans le module 'function'

Erreur : « gestionnaire » de méthode non défini pour #< > LambdaHandler:0x000055b76ccebf98

Erreur : aucune méthode publique nommée handleRequest avec la signature de méthode appropriée trouvée dans la classe function.Handler

Erreur : Impossible de trouver la méthode « HandleRequest » dans le type « » de l'assemblage « Function Function.Handler »

Le nom de la méthode du gestionnaire dans la configuration du gestionnaire de votre fonction ne correspond pas à votre code. Chaque environnement d'exécution définit une convention de dénomination pour les gestionnaires, telle que*`filename`*.*`methodname`*. Le gestionnaire correspond à la méthode dans le code de votre fonction que l'environnement d'exécution exécute lorsque la fonction est invoquée.

Pour certains langages, Lambda fournit une bibliothèque avec une interface pour laquelle une méthode de gestionnaire doit avoir un nom spécifique. Pour plus d'informations sur l'attribution de noms de gestionnaire pour chaque langue, consultez les rubriques suivantes.

- Création de fonctions événementielles Lambda avec Node.js
- Création de fonctions d'événement Lambda avec Python
- Création de fonctions d'événement Lambda avec Ruby
- Création de fonctions d'événement Lambda avec Java
- Création de fonctions événementielles Lambda avec Go
- Création de fonctions d'événement Lambda avec C#
- Création de fonctions d'événement Lambda avec PowerShell

Général : limite de stockage du code Lambda dépassée

Erreur : limite de stockage de code dépassée.

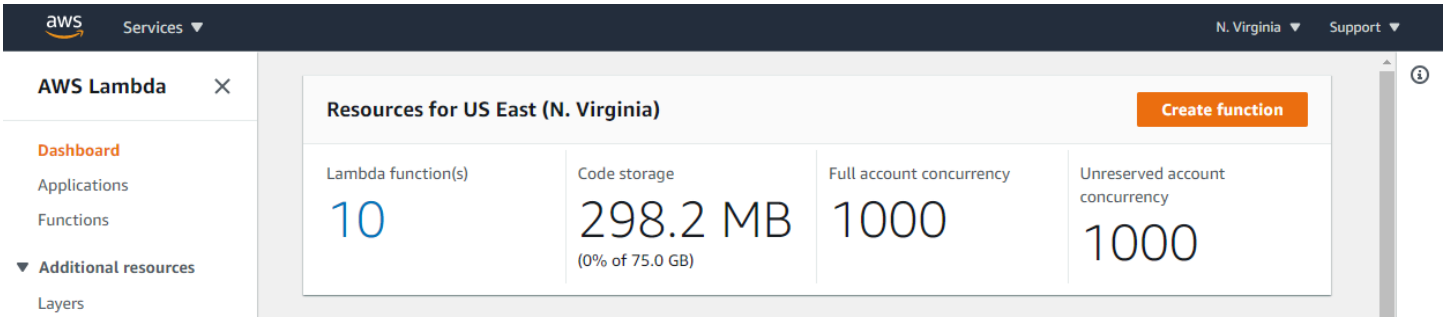
Lambda stocke une copie de votre code de fonction dans un compartiment S3 interne réservé à votre compte. Chaque AWS compte dispose de 300 Go de stockage de code (décompressé) dans chaque

région. Le stockage de code inclut le stockage total utilisé à la fois par les fonctions et les couches Lambda. Si vous atteignez le quota, vous recevez un CodeStorageExceededExceptionlorsque vous tentez de déployer de nouvelles fonctions.

Pour résoudre ce problème, vous pouvez nettoyer les anciennes versions des fonctions, supprimer le code inutilisé ou utiliser des couches Lambda pour dédupliquer le code commun partagé entre les fonctions. En outre, il est recommandé d'utiliser des AWS comptes distincts pour des charges de travail distinctes afin de gérer les quotas de stockage.

Vous pouvez également configurer vos fonctions et vos couches pour utiliser le stockage de code S3 autogéré. Grâce au stockage de code S3 autogéré, Lambda référence votre code directement à partir de votre compartiment S3, ce qui n'est pas pris en compte dans votre quota de stockage.

Vous pouvez consulter votre utilisation totale du stockage dans la console Lambda, dans le sous-menu Tableau de bord :



Lambda : échec de la conversion de couche

Erreur : la conversion de la couche Lambda a échoué. Pour obtenir des conseils sur la résolution de ce problème, consultez la page Résolution des problèmes de déploiement dans Lambda du Guide de l'utilisateur Lambda.

Lorsque vous configurez une fonction Lambda avec une couche, Lambda fusionne la couche avec le code de votre fonction. Si ce processus échoue, Lambda renvoie cette erreur. Si vous rencontrez cette erreur, réalisez les actions suivantes :

- Supprimer tous les fichiers inutiles de votre couche
- Supprimer tous les liens symboliques de votre couche
- Renommer tous les fichiers qui ont le même nom qu'un répertoire dans l'une des couches de votre fonction

Lambda : ou InvalidParameterValueException RequestEntityTooLargeException

Erreur InvalidParameterValueException : Lambda n'a pas pu configurer vos variables d'environnement car les variables d'environnement que vous avez fournies ont dépassé la limite de 4 Ko. Chaîne mesurée : {"A1" : « u... SFeY5cyPiPn7AtnX5BsM

Erreur RequestEntityTooLargeException : la demande doit être inférieure à 5120 octets pour l'opération UpdateFunctionConfiguration

La taille maximale de l’objet variable stocké dans la configuration de la fonction ne doit pas dépasser 4096 octets. Cela inclut les noms de clés, les valeurs, les guillemets, les virgules et les crochets. La taille totale du corps de requête HTTP est également limitée.

```
{
    "FunctionName": "my-function",
    "FunctionArn": "arn:aws:lambda:us-east-2:123456789012:function:my-function",
    "Runtime": "nodejs24.x",
    "Role": "arn:aws:iam::123456789012:role/lambda-role",
    "Environment": {
        "Variables": {
            "BUCKET": "amzn-s3-demo-bucket",
            "KEY": "file.txt"
        }
    },
    ...
}
```

Dans cet exemple, l’objet comporte 39 caractères et utilise 39 octets lorsqu’il est stocké (sans espace) comme chaîne `{"BUCKET":"amzn-s3-demo-bucket","KEY":"file.txt"}`. Les caractères ASCII standard dans les valeurs des variables d’environnement utilisent un octet chacun. Les caractères ASCII et Unicode étendus peuvent utiliser entre 2 et 4 octets par caractère.

Lambda : InvalidParameterValueException

Erreur InvalidParameterValueException : Lambda n'a pas pu configurer vos variables d'environnement car les variables d'environnement que vous avez fournies contiennent des clés réservées dont la modification n'est actuellement pas prise en charge.

Lambda réserve certaines clés de variables d’environnement pour une utilisation interne. Par exemple, `AWS_REGION` est utilisé par l’environnement d’exécution pour déterminer la région actuelle et ne peut pas être remplacé. D’autres variables, comme `PATH`, sont utilisées par l’environnement

d'exécution, mais peuvent être étendues dans la configuration de votre fonction. Pour obtenir une liste complète, veuillez consulter Variables d'environnement d'exécution définies.

Lambda : quotas de simultanéité et de mémoire

Erreur : la fonction spécifiée ConcurrentExecutions réduit le compte en UnreservedConcurrentExecution dessous de sa valeur minimale

Erreur : la valeur MemorySize « » n'a pas satisfait la contrainte : le membre doit avoir une valeur inférieure ou égale à 3008

Ces erreurs se produisent lorsque vous dépassez les quotas de simultanéité ou de mémoire pour votre compte. AWS Les nouveaux comptes ont réduit la simultanéité et les quotas de mémoire. Pour résoudre les erreurs liées à la simultanéité, vous pouvez demander une augmentation des quotas. Vous ne pouvez pas demander d'augmentation des quotas de mémoire.

- Simultanéité : vous pouvez recevoir un message d'erreur si vous essayez de créer une fonction à l'aide de la simultanéité réservée ou provisionnée, ou si votre demande de simultanéité par fonction (PutFunctionConcurrency) excède le quota de simultanéité de votre compte.
- Mémoire : des erreurs surviennent lorsque la capacité de mémoire allouée à la fonction dépasse le quota de mémoire de votre compte.

Lambda : configuration d'alias non valide pour la simultanéité provisionnée.

Erreur : configuration d'alias non valide pour la simultanéité provisionnée

Cette erreur se produit lorsque vous essayez de mettre à jour le code ou la configuration d'une fonction Lambda alors qu'un alias doté d'une simultanéité provisionnée pointe vers une version présentant des problèmes. Lambda pré-initialise les environnements d'exécution pour une simultanéité provisionnée, et si ces environnements ne peuvent pas être correctement initialisés en raison d'erreurs de code, de contraintes de ressources ou de l'utilisation d'une pile ou d'un alias affecté, le déploiement échoue. Si vous rencontrez ce problème, réalisez les actions suivantes :

1. Restaurer l'alias : mettez temporairement à jour l'alias pour qu'il pointe vers la version qui fonctionnait auparavant.

```
aws lambda update-alias \
 --function-name <function-name> \
 --name <alias-name> \
```

```
  --function-version <known-good-version>
```

2. Corriger le code d'initialisation Lambda : assurez-vous que le code d'initialisation exécuté en dehors du gestionnaire ne contient aucune exception non détectée et initialisez les clients et les connexions.
3. Redéployer de façon sûre : déployez le code corrigé et publiez une nouvelle version. Mettez ensuite à jour l'alias pour qu'il pointe vers la version corrigée. Réactivez éventuellement la simultanéité provisionnée, si nécessaire.

Si vous l'utilisez AWS CloudFormation, mettez à jour la définition de la pile `FunctionVersion:!GetAtt version.Version` afin que l'alias pointe vers la version de travail :

```
alias:
 Type: AWS::Lambda::Alias
 Properties:
 FunctionName: !Ref function
FunctionVersion: !GetAtt version.Version
 Name: BLUE
 ProvisionedConcurrencyConfig:
 ProvisionedConcurrentExecutions: 1
```

Résoudre les problèmes d'invocation dans Lambda

Lorsque vous appelez une fonction d'événement Lambda, Lambda valide la demande et vérifie le dimensionnement de la capacité avant d'envoyer l'événement à votre fonction ou, dans le cas d'un appel asynchrone, à la file d'attente d'événements. Les erreurs d'invocation peuvent être causées par des problèmes de paramètres de demande, de structure d'événement, de paramètres de fonction, d'autorisations utilisateur, d'autorisations de ressources ou de limites.

Si vous invoquez la fonction directement, les erreurs d'invocation sont visibles dans la réponse de Lambda. Si vous invoquez la fonction de manière asynchrone avec un mappage de source d'événement ou via un autre service, vous pouvez trouver des erreurs dans les journaux, une file d'attente de lettres mortes ou une destination en cas d'échec. Les options de gestion des erreurs et le comportement des nouvelles tentatives varient en fonction de la façon dont vous invoquez la fonction et du type d'erreur.

Pour obtenir la liste des types d'erreur que l'opération `Invoke` peut renvoyer, consultez Invoquer.

Rubriques

- Lambda : Expiration de la fonction pendant la phase d'initialisation () Sandbox.Timedout
- IAM : lambda : non autorisé InvokeFunction
- Lambda : Impossible de trouver bootstrap () valide Runtime.InvalidEntrypoint
- Lambda : L'opération ne peut pas être effectuée ResourceConflictException
- Lambda : La fonction est bloquée à l'état Pending (En attente)
- Lambda : Une fonction utilise toute la simultanéité
- Général : Impossible d'invoquer la fonction avec d'autres comptes ou services
- Général : L'invocation de la fonction boucle
- Lambda : Routage d'alias avec une simultanéité approvisionnée
- Lambda : Démarrages à froid avec la simultanéité allouée
- Lambda : Démarrages à froid avec de nouvelles versions
- Lambda : Node.js sortie inattendue lors de l'exécution () Runtime.NodejsExit
- EFS : La fonction n'a pas pu monter le système de fichiers EFS
- EFS : La fonction n'a pas pu se connecter au système de fichiers EFS
- EFS : La fonction n'a pas pu monter le système de fichiers EFS en raison d'une expiration de délai
- Fichiers S3 : la fonction n'a pas pu monter le système de fichiers S3
- Fichiers S3 : la fonction n'a pas pu se connecter au système de fichiers S3
- Fichiers S3 : la fonction n'a pas pu monter le système de fichiers S3 en raison d'un délai d'attente
- Lambda : Lambda a détecté un processus d'E/S qui prenait trop de temps
- Conteneur : CodeArtifactUserException erreurs
- Conteneur : InvalidEntrypoint erreurs

Lambda : Expiration de la fonction pendant la phase d'initialisation () Sandbox.Timedout

Erreur : Task timed out after 3.00 seconds

Lorsque la phase d'initialisation expire, Lambda initialise à nouveau l'environnement d'exécution en relançant la phase `Init` lorsque la prochaine demande d'invocation arrive. Cela s'appelle une init supprimée. Toutefois, si votre fonction est configurée avec un délai d'expiration court (généralement environ 3 secondes), l'initialisation supprimée risque de ne pas se terminer pendant le délai imparti, ce qui provoquera une nouvelle expiration de la phase `Init`. Sinon, l'initialisation supprimée se

termine mais ne laisse pas suffisamment de temps à la phase d'invocation pour se terminer, ce qui entraîne l'expiration de la phase `Invoke`.

Pour réduire les erreurs d'expiration, utilisez l'une des stratégies suivantes :

- Augmentez la durée du délai d'expiration de la fonction : prolongez le délai d'expiration pour donner aux phases `Invoke` et `Init` et le temps de se terminer.
- Augmentez l'allocation de mémoire de la fonction : plus de mémoire signifie également une allocation plus proportionnelle du processeur, ce qui peut accélérer à la fois les phases `Invoke` et `Init`.
- Optimisez le code d'initialisation de la fonction : réduisez le temps nécessaire à l'initialisation afin de garantir que les phases `Init` et `Invoke` puissent se terminer dans le délai configuré.

IAM : lambda : non autorisé InvokeFunction

Erreur : L'utilisateur : arn:aws:iam : :123456789012 : user/developer n'est pas autorisé à exécuter : lambda : on resource : my-function InvokeFunction

Votre utilisateur, ou le rôle que vous assumez, doit avoir une autorisation pour invoquer une fonction. Cette exigence s'applique également aux fonctions Lambda et à d'autres ressources de calcul qui invoquent des fonctions. Ajoutez la politique AWS gérée AWSLambdaRoleà votre utilisateur ou ajoutez une politique personnalisée qui autorise l'`lambda:InvokeFunction`action sur la fonction cible.

> **Note**
>
> Le nom de l'action IAM (`lambda:InvokeFunction`) fait référence à l'opération de l'API Lambda `Invoke`.

Pour plus d'informations, consultez Gestion des autorisations dans AWS Lambda.

Lambda : Impossible de trouver bootstrap () valide Runtime.InvalidEntrypoint

Erreur : Impossible de trouver un ou plusieurs bootstrap valides : [/var/task/bootstrap/] opt/bootstrap

Cette erreur se produit généralement lorsque la racine de votre package de déploiement ne contient pas de fichier exécutable nommé `bootstrap`. Par exemple, si vous déployez une fonction

`provided.al2023` avec un fichier .zip, le fichier `bootstrap` doit se trouver à la racine du fichier .zip, et non dans un répertoire.

Lambda : L'opération ne peut pas être effectuée ResourceConflictException

Erreur ResourceConflictException : Impossible d'effectuer l'opération pour le moment. La fonction est actuellement dans l'état suivant : En attente

Lorsque vous connectez une fonction à un cloud privé virtuel (Virtual Private Cloud, VPC) au moment de la création, la fonction passe à l'état `Pending` pendant que Lambda crée des interfaces réseau Elastic. Pendant ce temps, vous ne pouvez pas invoquer ni modifier votre fonction. Si vous connectez votre fonction à un VPC après la création, vous pouvez l'invoquer pendant que la mise à jour est en attente, mais vous ne pouvez pas modifier son code ni sa configuration.

Pour plus d'informations, consultez États de la fonction d'événement Lambda.

Lambda : La fonction est bloquée à l'état Pending (En attente)

Erreur : Une fonction est bloquée à l'état *`Pending`* depuis plusieurs minutes.

Si une fonction est bloquée à l'état `Pending` depuis plus de six minutes, appelez l'une des opérations d'API suivantes pour la débloquer :

- UpdateFunctionCode
- UpdateFunctionConfiguration
- PublishVersion

Lambda annule l'opération en attente et met la fonction à l'état `Failed`. Vous pouvez ensuite essayer une autre mise à jour.

Lambda : Une fonction utilise toute la simultanéité

Problème : une fonction utilise toute la simultanéité disponible, limitant ainsi d'autres fonctions.

Pour diviser la simultanéité disponible de votre AWS compte dans une AWS région en groupes, utilisez la simultanéité réservée. La simultanéité réservée garantit qu'une fonction s'adapte toujours à la simultanéité qui lui est assignée et qu'elle n'utilise pas plus de simultanéité que ce qui lui est attribué.

Général : Impossible d'invoquer la fonction avec d'autres comptes ou services

Problème : vous pouvez invoquer la fonction directement, mais elle ne s'exécute pas lorsqu'elle est invoquée par un autre service ou compte.

Vous accordez à d'autres services et comptes l'autorisation d'invoquer une fonction dans la stratégie basée sur les ressourcesde la fonction. Si l'appelant se trouve dans un autre compte, cet utilisateur doit également avoir l'autorisation d'invoquer des fonctions.

Général : L'invocation de la fonction boucle

Problème : La fonction est invoquée en continu dans une boucle.

Cela se produit généralement lorsque votre fonction gère les ressources du même AWS service qui la déclenche. Par exemple, il est possible de créer une fonction qui stocke un objet dans un compartiment Amazon Simple Storage Service (Amazon S3) configuré avec une notification qui invoque à nouveau la fonction. Pour arrêter l'exécution de la fonction, réduisez la simultanéité disponible de votre fonction à zéro, ce qui limite toutes les invocations futures.

Identifiez ensuite le chemin de code ou l'erreur de configuration qui a provoqué l'invocation récursive. Lambda détecte et arrête automatiquement les boucles récursives pour certains AWS services et SDK. Pour plus d'informations, consultez the section called "Détection de boucle récursive".

Lambda : Routage d'alias avec une simultanéité approvisionnée

Problème: invocations de débordement de simultanéité approvisionnée pendant le routage d'alias.

Lambda utilise un modèle probabiliste simple pour distribuer le trafic entre les deux versions de la fonction. Quand le niveau de trafic est faible, il se peut que vous observiez une variance élevée entre les pourcentages de trafic configuré et réel sur chaque version. Si votre fonction utilise une simultanéité approvisionnée, vous pouvez éviter des invocations de débordement en configurant un plus grand nombre d'instances de simultanéité approvisionnées pendant que le routage d'alias est actif.

Lambda : Démarrages à froid avec la simultanéité allouée

Problème : Vous remarquez des démarrages à froid après avoir activé la simultanéité allouée.

Lorsque le nombre d'exécutions simultanées sur une fonction est inférieur ou égal au niveau de simultanéité configuré, il ne devrait pas y avoir de démarrage à froid. Pour vous aider à vérifier le bon fonctionnement de la simultanéité, procédez comme suit :

- Vérifiez que la simultanéité allouée est activée sur la version de fonction ou l'alias.

> **Note**
>
> La simultanéité allouée n'est pas configurable sur la version non publiée de la fonction ($LATEST).

- Assurez-vous que vos déclencheurs invoquent la version ou l'alias de fonction correct. Par exemple, si vous utilisez Amazon API Gateway, vérifiez qu'API Gateway invoque la version de fonction ou l'alias avec la simultanéité approvisionnée, et non $LATEST. Pour confirmer que la simultanéité provisionnée est utilisée, vous pouvez consulter la métrique ProvisionedConcurrencyInvocations Amazon CloudWatch . Une valeur non nulle indique que la fonction traite des invocations sur les environnements d'exécution initialisés.
- Déterminez si la simultanéité de vos fonctions dépasse le niveau configuré de simultanéité provisionnée en vérifiant la métrique. ProvisionedConcurrencySpilloverInvocations CloudWatch Une valeur différente de zéro indique que toute la simultanéité allouée est en cours d'utilisation et qu'une invocation s'est produite avec un démarrage à froid.
- Vérifiez la fréquence des invocations (demandes par seconde). Les fonctions avec simultanéité allouée ont un taux maximal de 10 demandes par seconde par simultanéité allouée. Par exemple, une fonction configurée avec une simultané allouée de 100 peut traiter 1 000 demandes par seconde. Si le taux d'invocations dépasse 1 000 requêtes par seconde, certains démarrages à froid peuvent se produire.

Lambda : Démarrages à froid avec de nouvelles versions

Problème : Vous notez des démarrages à froid lors du déploiement de nouvelles versions de votre fonction.

Lorsque vous mettez à jour un alias de fonction, Lambda déplace automatiquement la simultanéité approvisionnée vers la nouvelle version en fonction des pondérations configurées sur l'alias.

Erreur KMSDisabledException : Lambda n'a pas pu déchiffrer les variables d'environnement car la clé KMS utilisée est désactivée. Veuillez vérifier les paramètres de clé KMS de la fonction.

Cette erreur peut se produire si votre clé AWS Key Management Service (AWS KMS) est désactivée ou si l'autorisation permettant à Lambda d'utiliser la clé est révoquée. Si l'octroi est manquant, configurez la fonction pour utiliser une autre clé. Ensuite, réaffectez la clé personnalisée pour recréer l'octroi.

Lambda : Node.js sortie inattendue lors de l'exécution () Runtime.NodejsExit

Problème : le client d'exécution Lambda a détecté un code de Node.js sortie inattendu.

Cette erreur se produit lorsque votre fonction se ferme avant que toutes les promesses ne soient réglées, par exemple en raison d'un bogue de code. Cela peut également se produire lors Node.js de la détection d'un blocage empêchant le règlement des promesses. Cette erreur affecte uniquement les gestionnaires de style asynchrone, pas les gestionnaires de style rappel.

Runtimes concernés : Node.js 18 et versions ultérieures.

Pour résoudre ce problème :

1. Vérifiez que le code de votre fonction ne contient pas de promesses non réglées dans les gestionnaires asynchrones.
2. Assurez-vous que toutes les promesses sont correctement réglées (résolues ou rejetées) avant la fin de la fonction.
3. Vérifiez votre code pour détecter les conditions de course potentielles lors d'opérations asynchrones.

Pour plus d'informations sur les codes de Node.js sortie et la fin du processus, consultez la Node.js documentation.

EFS : La fonction n’a pas pu monter le système de fichiers EFS

Erreur EFSMountFailureException : La fonction n'a pas pu monter le système de fichiers EFS avec le point d'accès arn:aws:elasticfilesystem:us-east - 2:123456789012:access- -015cxmplb72b405fd. point/fsap

La demande de montage sur le système de fichiers de la fonction a été rejetée. Vérifiez les autorisations de la fonction et confirmez que son système de fichiers et son point d’accès existent et sont prêts à l’emploi.

EFS : La fonction n’a pas pu se connecter au système de fichiers EFS

Erreur EFSMountConnectivityException : La fonction n'a pas pu se connecter au système de fichiers Amazon EFS avec le point d'accès arn:aws:elasticfilesystem:us-east - 2:123456789012:access- -015cxmplb72b405fd. point/fsap Vérifiez la configuration de votre réseau et réessayez.

La fonction n’a pas pu établir de connexion au système de fichiers de la fonction avec le protocole NFS (port TCP 2049). Vérifiez le groupe de sécurité et la configuration de routage pour les sous-réseaux du VPC.

Si vous rencontrez ces erreurs après avoir mis à jour les paramètres de configuration VPC de votre fonction, essayez de démonter puis de remonter le système de fichiers.

EFS : La fonction n’a pas pu monter le système de fichiers EFS en raison d’une expiration de délai

Erreur EFSMountTimeoutException : La fonction n'a pas pu monter le système de fichiers EFS avec le point d'accès {arn:aws:elasticfilesystem:us-east - 2:123456789012:access- -015cxmplb72b405fd} en raison d'un délai de montage dépassé. point/fsap

La fonction a pu se connecter au système de fichiers de la fonction, mais l’opération de montage a expiré. Réessayez après un court laps de temps et envisagez de limiter la concurrence de la fonction pour réduire la charge sur le système de fichiers.

Fichiers S3 : la fonction n'a pas pu monter le système de fichiers S3

Erreur : S3FilesMountFailureException : La fonction n'a pas pu monter le système de fichiers Amazon S3 avec le point d'accès arn:aws:s3files:us-east - 2:123456789012:access- -123456789abcde. point/fsap

La demande de montage sur le système de fichiers de la fonction a été rejetée. Vérifiez les autorisations de la fonction et confirmez que son système de fichiers et son point d’accès existent et sont prêts à l’emploi.

Fichiers S3 : la fonction n'a pas pu se connecter au système de fichiers S3

Erreur : S3FilesMountConnectivityException : La fonction n'a pas pu se connecter au système de fichiers Amazon S3 avec le point d'accès arn:aws:s3files:us-east - 2:123456789012:access- -123456789abcde. point/fsap Vérifiez la configuration de votre réseau et réessayez.

La fonction n’a pas pu établir de connexion au système de fichiers de la fonction avec le protocole NFS (port TCP 2049). Vérifiez le groupe de sécurité et la configuration de routage pour les sous-réseaux du VPC.

Si vous rencontrez ces erreurs après avoir mis à jour les paramètres de configuration VPC de votre fonction, essayez de démonter puis de remonter le système de fichiers.

Fichiers S3 : la fonction n'a pas pu monter le système de fichiers S3 en raison d'un délai d'attente

Erreur S3FilesMountTimeoutException : La fonction n'a pas pu monter le système de fichiers S3 avec le point d'accès {arn:aws:s3files:us-east- 2:123456789012:access- -123456789abcde} en raison d'un délai de montage dépassé. point/fsap

La fonction a pu se connecter au système de fichiers de la fonction, mais l'opération de montage a expiré. Réessayez après un court laps de temps et envisagez de limiter la concurrence de la fonction pour réduire la charge sur le système de fichiers.

Lambda : Lambda a détecté un processus d'E/S qui prenait trop de temps

EFSIOException : cette instance de fonction a été arrêtée car Lambda a détecté un processus d'E/S qui prenait trop de temps.

Une invocation précédente a expiré et Lambda n'a pas pu mettre fin à l'exécution du gestionnaire de fonction. Ce problème peut se produire lorsqu'un système de fichiers joint manque de crédits de rafale et que le débit de base est insuffisant. Pour augmenter le débit, vous pouvez augmenter la taille du système de fichiers ou utiliser le débit provisionné.

Conteneur : CodeArtifactUserException erreurs

Erreur : message CodeArtifactUserPendingException d'erreur

L'optimisation CodeArtifact est en attente. La fonction passera à l'état Actif lorsque Lambda aura terminé l'optimisation. Code de réponse HTTP : 409.

Erreur : message CodeArtifactUserDeletedException d'erreur

CodeArtifact Il est prévu de le supprimer. Code de réponse HTTP : 409.

Erreur : message CodeArtifactUserFailedException d'erreur

Lambda n'a pas réussi à optimiser le code. Vous devez corriger le code et le charger à nouveau. Code de réponse HTTP : 409.

Conteneur : InvalidEntrypoint erreurs

Erreur : Runtime.ExitError ou « ErrorType » : "" Runtime.InvalidEntrypoint

Vérifiez que l'ENTRYPOINT de votre image de conteneur inclut le chemin absolu comme emplacement. Vérifiez également que l'image ne contient pas de lien symbolique en tant qu'ENTRYPOINT.

Erreur : vous utilisez un CloudFormation modèle et votre conteneur ENTRYPOINT est remplacé par une valeur nulle ou vide.

Passez en revue la ImageConfigressource dans le CloudFormation modèle. Si vous déclarez une ressource `ImageConfig` dans votre modèle, vous devez fournir des valeurs non vides pour les trois propriétés.

Résoudre les problèmes d’exécution dans Lambda

Lorsque le moteur d'exécution Lambda exécute votre code de fonction, l'événement peut être traité sur une instance de la fonction d'événement Lambda qui traite des événements depuis un certain temps, ou il peut nécessiter l'initialisation d'une nouvelle instance. Des erreurs peuvent se produire lors de l’initialisation de la fonction, lorsque le code de gestionnaire traite l’événement ou lorsque la fonction renvoie (ou ne parvient pas à renvoyer) une réponse.

Les erreurs d’exécution de fonction peuvent être causées par des problèmes de code, de configuration de fonction, de ressources en aval ou d’autorisations. Si vous appelez la fonction directement, les erreurs de fonction sont visibles dans la réponse de Lambda. Si vous appelez la fonction de manière asynchrone, avec un mappage de source d’événement ou via un autre service, vous pouvez trouver les erreurs dans les journaux, une file d’attente de lettres mortes ou une destination réservées aux échecs. Les options de gestion des erreurs et le comportement des nouvelles tentatives varient en fonction de la façon dont vous appelez la fonction et du type d’erreur.

Lorsque le code de fonction ou le runtime Lambda renvoient une erreur, le code d’état indiqué dans la réponse de Lambda est 200 OK. La présence d’une erreur dans la réponse est indiquée par un en-tête nommé `X-Amz-Function-Error`. Les codes d’état des séries 400 et 500 sont réservés aux erreurs d’invocation.

Rubriques

- Lambda : débogage à distance avec Visual Studio Code
- Lambda : l’exécution prend trop de temps
- Lambda : données utiles d’événement imprévu
- Lambda : données utiles plus volumineuses qu’attendu
- Lambda : erreurs de codage et de décodage JSON

- Lambda : les journaux ou les traces n'apparaissent pas
- Lambda : certains journaux de ma fonction n'apparaissent pas
- Lambda : la fonction renvoie avant la fin de l'exécution
- Lambda : exécution d'une version ou d'un alias de fonction imprévu
- Lambda : détection de boucles infinies
- Général : indisponibilité du service en aval
- AWS SDK : versions et mises à jour
- Python : les bibliothèques se chargent de manière incorrecte
- Java : votre fonction met plus de temps à traiter les événements après la mise à jour de Java 11 vers Java 17
- Kafka : Problèmes de gestion des erreurs et de configuration des nouvelles tentatives

Lambda : débogage à distance avec Visual Studio Code

Problème : difficulté à résoudre les problèmes liés au comportement complexe des fonctions Lambda dans l'environnement réel AWS

Lambda fournit une fonctionnalité de débogage à distance via AWS Toolkit for Visual Studio Code. Pour instructions générales et de configuration, consultez Déboguer à distance les fonctions d'événement Lambda avec Visual Studio Code.

Pour obtenir des instructions détaillées sur le dépannage, les cas d'utilisation avancés et la disponibilité régionale, consultez la section Débogage à distance des fonctions Lambda dans AWS Toolkit for Visual Studio Code le guide de l'utilisateur.

Lambda : l'exécution prend trop de temps

Problème : l'exécution de la fonction prend trop de temps.

Si votre code met beaucoup plus de temps à s'exécuter dans Lambda que sur votre machine locale, il est possible qu'il soit limité par la mémoire ou la puissance de traitement disponible pour la fonction. Configurez la fonction avec de la mémoire supplémentaire pour augmenter à la fois la mémoire et la capacité d'UC.

Lambda : données utiles d'événement imprévu

Problème : erreurs de fonctionnement liées à du JSON mal formé ou à une validation inadéquate des données.

Toutes les fonctions Lambda reçoivent des données utiles d'événement dans le premier paramètre du gestionnaire. La charge utile de l'événement est une structure JSON qui peut contenir des tableaux et des éléments imbriqués.

Un JSON mal formé peut se produire lorsqu'il est fourni par des services en amont qui n'utilisent pas de processus robuste pour vérifier les structures JSON. Cela se produit lorsque les services concatènent des chaînes de texte ou intègrent des entrées utilisateur qui n'ont pas été nettoyées. Le JSON est également fréquemment sérialisé pour le transfert d'un service à l'autre. Analysez toujours les structures JSON en tant que producteur et consommateur de JSON pour vous assurer que la structure est valide.

De même, le fait de ne pas vérifier les plages de valeurs dans les données utiles de l'événement peut entraîner des erreurs. L'exemple suivant montre une fonction qui calcule une retenue d'impôt :

```
exports.handler = async (event) => {
    let pct = event.taxPct
    let salary = event.salary

    // Calculate % of paycheck for taxes
    return (salary * pct)
}
```

Cette fonction utilise un salaire et un taux d'imposition issus des données utiles de l'événement pour effectuer le calcul. Cependant, le code ne vérifie pas si les attributs sont présents. Il ne vérifie pas non plus les types de données ou ne garantit pas les limites, par exemple en s'assurant que le pourcentage de taxe est compris entre 0 et 1. Par conséquent, les valeurs situées en dehors de ces limites produisent des résultats absurdes. Un type incorrect ou un attribut manquant provoque une erreur d'exécution.

Créez des tests pour vous assurer que votre fonction gère des données utiles plus importantes. La taille maximale des données utiles d'un événement Lambda est de 1 Mo. Selon le contenu, des charges utiles plus importantes peuvent entraîner la transmission d'un plus grand nombre d'éléments à la fonction ou l'intégration d'un plus grand nombre de données binaires dans un attribut JSON. Dans les deux cas, cela peut entraîner un traitement supplémentaire pour une fonction Lambda.

Des données utiles plus importantes peuvent également entraîner des délais d'expiration. Par exemple, une fonction Lambda traite un enregistrement toutes les 100 ms et son délai d'expiration est de 3 secondes. Le traitement est réussi pour 0 à 29 éléments des données utiles. Cependant, une fois que les données utiles contiennent plus de 30 éléments, la fonction expire et génère une erreur.

Pour éviter cela, assurez-vous que les délais sont définis de manière à gérer le temps de traitement supplémentaire pour le nombre maximal d'éléments attendus.

Lambda : données utiles plus volumineuses qu'attendu

Problème : les fonctions expirent ou provoquent des erreurs en raison de données utiles volumineuses.

Des données utiles plus importantes peuvent entraîner des expirations de délai et des erreurs. Nous vous recommandons de créer des tests pour vous assurer que votre fonction gère les données utiles attendues les plus importantes et vous assurer que le délai d'expiration de la fonction est correctement défini.

Par ailleurs, certaines données utiles d'événements peuvent contenir des pointeurs vers d'autres ressources. Par exemple, une fonction Lambda dotée de 128 Mo de mémoire peut effectuer un traitement d'image sur un fichier JPG stocké sous forme d'objet dans S3. La fonction fonctionne comme prévu avec des fichiers image plus petits.

Toutefois, lorsqu'un fichier JPG plus volumineux est fourni en entrée, la fonction Lambda génère une erreur en raison d'un manque de mémoire. Pour éviter cela, les cas de test doivent inclure des exemples tirés des limites supérieures des tailles de données attendues. Le code doit également valider les tailles des données utiles.

Lambda : erreurs de codage et de décodage JSON

Problème : NoSuchKey exception lors de l'analyse des entrées JSON.

Vérifiez que vous traitez correctement les attributs JSON. Par exemple, pour les événements générés par S3, l'attribut `s3.object.key` contient un nom de clé d'objet codé par URL. De nombreuses fonctions traitent cet attribut sous forme de texte pour charger l'objet S3 référencé :

Example

```
const originalText = await s3.getObject({
  Bucket: event.Records[0].s3.bucket.name,
  Key: event.Records[0].s3.object.key
}).promise()
```

Ce code fonctionne avec le nom de clé `james.jpg`, mais génère une erreur `NoSuchKey` lorsque le nom est `james beswick.jpg`. Étant donné que le codage URL convertit les espaces et les autres

caractères d'un nom de clé, vous devez vous assurer que les fonctions décodent les clés avant d'utiliser ces données :

Example

```
const originalText = await s3.getObject({
  Bucket: event.Records[0].s3.bucket.name,
  Key: decodeURIComponent(event.Records[0].s3.object.key.replace(/\+/g, " "))
}).promise()
```

Lambda : les journaux ou les traces n'apparaissent pas

Problème : les journaux n'apparaissent pas dans CloudWatch les journaux.

Problème : les traces n'apparaissent pas dans AWS X-Ray.

Votre fonction doit être autorisée à appeler CloudWatch Logs et X-Ray. Mettez à jour son rôle d'exécution pour lui accorder l'autorisation. Ajoutez les stratégies gérées suivantes pour activer les journaux et le suivi.

- AWSLambdaBasicExecutionRole
- AWSXRayDaemonWriteAccess

Lorsque vous ajoutez des autorisations à votre fonction, modifiez légèrement son code ou sa configuration. Cela force l'arrêt et le remplacement des instances en cours d'exécution de votre fonction, qui ont des informations d'identification obsolètes.

> **Note**
>
> L'affichage des journaux peut prendre de 5 à 10 minutes après l'invocation d'une fonction.

Lambda : certains journaux de ma fonction n'apparaissent pas

Problème : les journaux des fonctions sont absents dans CloudWatch les journaux, même si mes autorisations sont correctes

Si vous atteignez Compte AWS les limites de quota de CloudWatch journalisation, CloudWatch les régulateurs fonctionnent à la journalisation. Dans ce cas, certains journaux générés par vos fonctions peuvent ne pas apparaître dans CloudWatch les journaux.

Si votre fonction produit des journaux à un taux trop élevé pour que Lambda puisse les traiter, cela peut également empêcher les sorties des journaux d'apparaître dans CloudWatch les journaux. Lorsque Lambda ne parvient pas à envoyer des journaux CloudWatch au rythme auquel votre fonction les produit, il supprime les journaux pour empêcher l'exécution de votre fonction de ralentir. Attendez-vous à observer régulièrement la perte de journaux lorsque votre débit de journaux dépasse 2 MB/s pour un seul flux de journaux.

Si votre fonction est configurée pour utiliser des journaux au format JSON, Lambda essaie d'envoyer `logsDropped`un événement CloudWatch à Logs lorsqu'il supprime des journaux. Toutefois, lorsque vous CloudWatch limitez la journalisation de votre fonction, cet événement risque de ne pas atteindre les CloudWatch journaux. Vous ne verrez donc pas toujours d'enregistrement lorsque Lambda supprime les journaux.

Pour vérifier si votre quota de CloudWatch logs Compte AWS est atteint, procédez comme suit :

1. Ouvrez la console Service Quotas.
2. Dans le panneau de navigation, choisissez Services AWS .
3. Dans la liste des AWS services, recherchez Amazon CloudWatch Logs.
4. Dans la liste des quotas de service, choisissez les quotas `CreateLogGroup throttle limit in transactions per second`, `CreateLogStream throttle limit in transactions per second` et `PutLogEvents throttle limit in transactions per second` pour afficher votre utilisation.

Vous pouvez également configurer des CloudWatch alarmes pour vous avertir lorsque l'utilisation de votre compte dépasse la limite que vous avez spécifiée pour ces quotas. Pour en savoir plus, reportez-vous à la section Création d'une CloudWatch alarme basée sur un seuil statique.

Si les limites de quota par défaut pour CloudWatch les journaux ne sont pas suffisantes pour votre cas d'utilisation, vous pouvez demander une augmentation du quota.

Lambda : la fonction renvoie avant la fin de l’exécution

Problème : (Node.js) La fonction revient avant la fin de l'exécution du code

De nombreuses bibliothèques, y compris le AWS SDK, fonctionnent de manière asynchrone. Lorsque vous effectuez un appel réseau ou toute autre opération nécessitant l’attente d’une réponse, les bibliothèques renvoient un objet appelé promesse, qui suit la progression de l’opération en arrière-plan.

Pour attendre que la promesse soit résolue en réponse, utilisez le mot-clé `await`. Celui-ci empêche le code de gestionnaire de s'exécuter jusqu'à ce que la promesse soit résolue en objet contenant la réponse. Si vous n'avez pas besoin d'utiliser les données de la réponse dans votre code, vous pouvez retourner la promesse directement à l'environnement d'exécution.

Certaines bibliothèques ne retournent pas de promesses, mais peuvent être enveloppées dans du code qui le fait. Pour plus d'informations, consultez Définissez le gestionnaire de fonctions d'événement Lambda dans Node.js.

Lambda : exécution d'une version ou d'un alias de fonction imprévu

Problème : la version ou l'alias de la fonction n'est pas invoqué

Lorsque vous publiez de nouvelles fonctions Lambda dans la console ou que vous utilisez AWS SAM, la dernière version du code est représentée par. `$LATEST` Par défaut, les invocations qui ne spécifient pas de version ou d'alias ciblent automatiquement la version `$LATEST` du code de votre fonction.

Si vous utilisez des versions de fonction ou des alias spécifiques, il s'agit de versions publiées immuables d'une fonction en plus de `$LATEST`. Lors du dépannage de ces fonctions, déterminez d'abord si l'appelant a invoqué la version ou l'alias souhaité. Vous pouvez le faire en consultant vos journaux de fonction. La version de la fonction qui a été invoquée est toujours affichée dans la ligne de journal START :

```
2020-11-13T09:53:21.179-05:00          START RequestId: a37400cb-f3bc-441b-8592-dcb9fa552995 Version: 1

2020-11-13T08:14:27.834-05:00          START RequestId: f4943cb9-58a1-472a-af81-5801b6f0eb8d Version: $LATEST
```

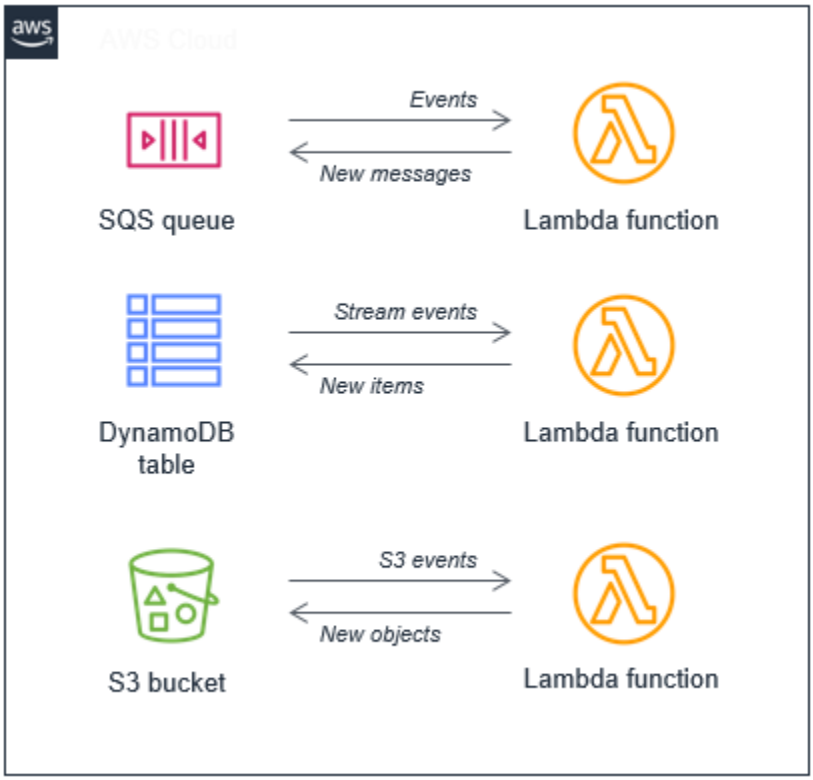
Lambda : détection de boucles infinies

Problème : modèles de boucles infinis liés aux fonctions Lambda

Il existe deux types de boucles infinies dans les fonctions Lambda. Le premier se trouve dans la fonction elle-même, à cause d'une boucle qui ne sort jamais. L'invocation prend fin uniquement lorsque la fonction expire. Vous pouvez identifier ces boucles en surveillant les expirations de délai, puis en corrigeant le comportement de bouclage.

Le second type de boucle se situe entre les fonctions Lambda et les autres AWS ressources. Elles se produisent lorsqu'un événement provenant d'une ressource telle qu'un compartiment S3 appelle

une fonction Lambda, qui interagit ensuite avec la même ressource source pour déclencher un autre événement. Cela invoque à nouveau la fonction, qui crée une autre interaction avec le même compartiment S3, et ainsi de suite. Ces types de boucles peuvent être provoqués par différentes sources d' AWS événements, notamment les files d'attente Amazon SQS et les tables DynamoDB. Vous pouvez utiliser la détection de boucle récursive pour identifier ces modèles.



Vous pouvez éviter ces boucles en veillant à ce que les fonctions Lambda écrivent dans des ressources différentes de celles qui les consomment. Si vous devez republier les données sur la ressource consommatrice, assurez-vous que les nouvelles données ne déclenchent pas le même événement. Vous pouvez également utiliser le filtrage des événements. Par exemple, voici deux solutions proposées pour les boucles infinies avec les ressources S3 et DynamoDB :

- Si vous réécrivez dans le même compartiment S3, utilisez un préfixe ou un suffixe différent de celui du déclencheur d'événement.
- Si vous écrivez des éléments dans la même table DynamoDB, incluez un attribut sur lequel une fonction Lambda consommatrice peut filtrer. Si Lambda trouve l'attribut, il n'en résultera aucune autre invocation.

Général : indisponibilité du service en aval

Problème : les services en aval sur lesquels repose votre fonction Lambda ne sont pas disponibles

Pour les fonctions Lambda qui font appel à des points de terminaison tiers ou à d'autres ressources en aval, assurez-vous qu'elles sont capables de gérer les erreurs de service et les délais d'expiration. Ces ressources en aval peuvent avoir des temps de réponse variables ou devenir indisponibles en raison d'interruptions de service. Selon l'implémentation, ces erreurs en aval peuvent apparaître sous forme de délais Lambda ou d'exceptions si la réponse d'erreur du service n'est pas gérée dans le code de fonction.

Chaque fois qu'une fonction dépend d'un service en aval, tel qu'un appel d'API, implémentez une gestion des erreurs et une logique de nouvelle tentative appropriées. Pour les services critiques, la fonction Lambda doit publier des métriques ou des journaux sur. CloudWatch Par exemple, si une API de paiement tierce n'est plus disponible, votre fonction Lambda peut journaliser ces informations. Vous pouvez ensuite configurer des CloudWatch alarmes pour envoyer des notifications relatives à ces erreurs.

Comme Lambda peut évoluer rapidement, les services en aval non sans serveur peuvent avoir du mal à gérer les pics de trafic. Il existe trois approches courantes pour gérer ce problème :

- Mise en cache : envisagez de mettre en cache le résultat des valeurs renvoyées par des services tiers si elles ne changent pas fréquemment. Vous pouvez stocker ces valeurs dans une variable globale, dans votre fonction ou dans un autre service. Par exemple, les résultats d'une requête de liste de produits provenant d'une instance Amazon RDS peuvent être enregistrés pendant un certain temps dans la fonction afin d'éviter les requêtes redondantes.
- Mise en file d'attente : lors de l'enregistrement ou de la mise à jour de données, ajoutez une file d'attente Amazon SQS entre la fonction Lambda et la ressource. La file d'attente conserve les données de manière durable pendant que le service en aval traite les messages.
- Proxies : lorsque des connexions de longue durée sont généralement utilisées, comme pour les instances Amazon RDS, utilisez une couche proxy pour regrouper et réutiliser ces connexions. Pour les bases de données relationnelles, Amazon RDS Proxy est un service conçu pour améliorer l'évolutivité et la résilience des applications. Lambda-based

AWS SDK : versions et mises à jour

Problème : le AWS SDK inclus dans le moteur d'exécution n'est pas la dernière version

Problème : le AWS SDK inclus dans le moteur d'exécution est automatiquement mis à jour

Les environnements d'exécution pour les langages interprétés incluent une version du AWS SDK. Lambda met régulièrement à jour ces environnements d'exécution pour utiliser la dernière version du SDK. Pour trouver la version du SDK incluse dans votre environnement d'exécution, consultez les sections suivantes :

- Versions du SDK incluses dans l'environnement d'exécution () Node.js
- Versions du SDK incluses dans l'environnement d'exécution (Python)
- Versions du SDK incluses dans l'environnement d'exécution (Ruby)

Pour utiliser une version plus récente du AWS SDK ou pour verrouiller vos fonctions sur une version spécifique, vous pouvez regrouper la bibliothèque avec votre code de fonction ou créer une couche Lambda. Pour plus d'informations sur la création d'un package de déploiement avec des dépendances, consultez les rubriques suivantes :

Node.js

Déployez les fonctions d'événement Node.js Lambda avec des archives de fichiers .zip

Python

Utilisation d'archives de fichiers .zip pour les fonctions événementielles Lambda en Python

Ruby

Déployez les fonctions d'événement Ruby Lambda avec des archives de fichiers .zip

Java

Déployez les fonctions d'événement Java Lambda avec des archives de fichiers .zip ou JAR

Go

Déployez les fonctions d'événement Go Lambda avec des archives de fichiers .zip

C#

Créez et déployez des fonctions d'événement Lambda C# avec des archives de fichiers .zip

PowerShell

Déployez les fonctions d'événement PowerShell Lambda avec des archives de fichiers .zip

Python : les bibliothèques se chargent de manière incorrecte

Problème : (Python) certaines bibliothèques ne se chargent pas correctement à partir du package de déploiement

Les bibliothèques avec des modules d'extension écrits en C ou C++ doivent être compilées dans un environnement avec la même architecture de processeur que Lambda (Amazon Linux). Pour plus d'informations, consultez Utilisation d'archives de fichiers .zip pour les fonctions événementielles Lambda en Python.

Java : votre fonction met plus de temps à traiter les événements après la mise à jour de Java 11 vers Java 17

Probème : (Java) votre fonction met plus de temps à traiter les événements après la mise à jour de Java 11 vers Java 17

Réglez votre compilateur à l'aide du paramètre `JAVA_TOOL_OPTIONS`. Les environnements d'exécution Lambda pour Java 17 et versions ultérieures modifient les options du compilateur par défaut. Cette modification améliore les temps de démarrage à froid pour les fonctions de courte durée, mais le comportement précédent est mieux adapté aux fonctions de longue durée gourmandes en calcul. Définissez `JAVA_TOOL_OPTIONS` sur `-XX:-TieredCompilation` pour revenir au comportement de Java 11. Pour plus d'informations sur le paramètre `JAVA_TOOL_OPTIONS`, consultez the section called "Comprendre la variable d'environnement `JAVA_TOOL_OPTIONS`".

Kafka : Problèmes de gestion des erreurs et de configuration des nouvelles tentatives

Problème : le mappage de la source d'événements Kafka ne parvient pas à configurer les paramètres de nouvelle tentative ou les destinations en cas d'échec

Les configurations de nouvelle tentative de Kafka et les destinations en cas d'échec ne sont disponibles que pour les mappages de sources d'événements avec le mode provisionné activé. Assurez-vous d'avoir configuré votre configuration `ProvisionedPollerConfig` avant `MinimumPollers` de tenter de définir des configurations de nouvelle tentative.

Erreurs de configuration courantes :

- Nombre infini de tentatives avec un lot divisé en deux : vous ne pouvez pas l'activer `BisectBatchOnFunctionError` lorsque `MaximumRetryAttempts` ce paramètre est défini sur -1 (infini). Définissez une limite de tentatives limitée ou désactivez le traitement par lots en deux.

- Récursivité sur le même sujet — Le sujet de destination de Kafka en cas d'échec ne peut être identique à aucun de vos sujets source. Choisissez un autre nom de sujet pour votre sujet lettre morte.
- Format de destination Kafka non valide : utilisez le `kafka://<topic-name>` format lorsque vous spécifiez un sujet Kafka comme destination en cas d'échec.
- kafka : problèmes WriteData d'autorisation — Assurez-vous que votre rôle d'exécution dispose `kafka-cluster:WriteData` des autorisations pour le sujet de destination. Le sujet n'existe pas. Les exceptions de délai d'expiration ou les problèmes de limitation de l'API d'écriture peuvent nécessiter une augmentation des limites du compte.

Résoudre les problèmes de mappage des sources d’événements dans Lambda

Dans Lambda, les problèmes liés au mappage des sources d’événements peuvent être plus complexes, car ils impliquent le débogage sur plusieurs services. De plus, le comportement de la source d’événements peut différer en fonction de la source d’événements exacte utilisée. Cette section répertorie les problèmes courants liés aux mappages des sources d’événements et fournit des conseils sur la manière de les identifier et de les résoudre.

> **Note**
>
> Cette section utilise une source d'événements Amazon SQS à titre d'illustration, mais les principes s'appliquent aux autres mappages de sources d'événements qui mettent en file d'attente des messages pour Lambda Event Functions.

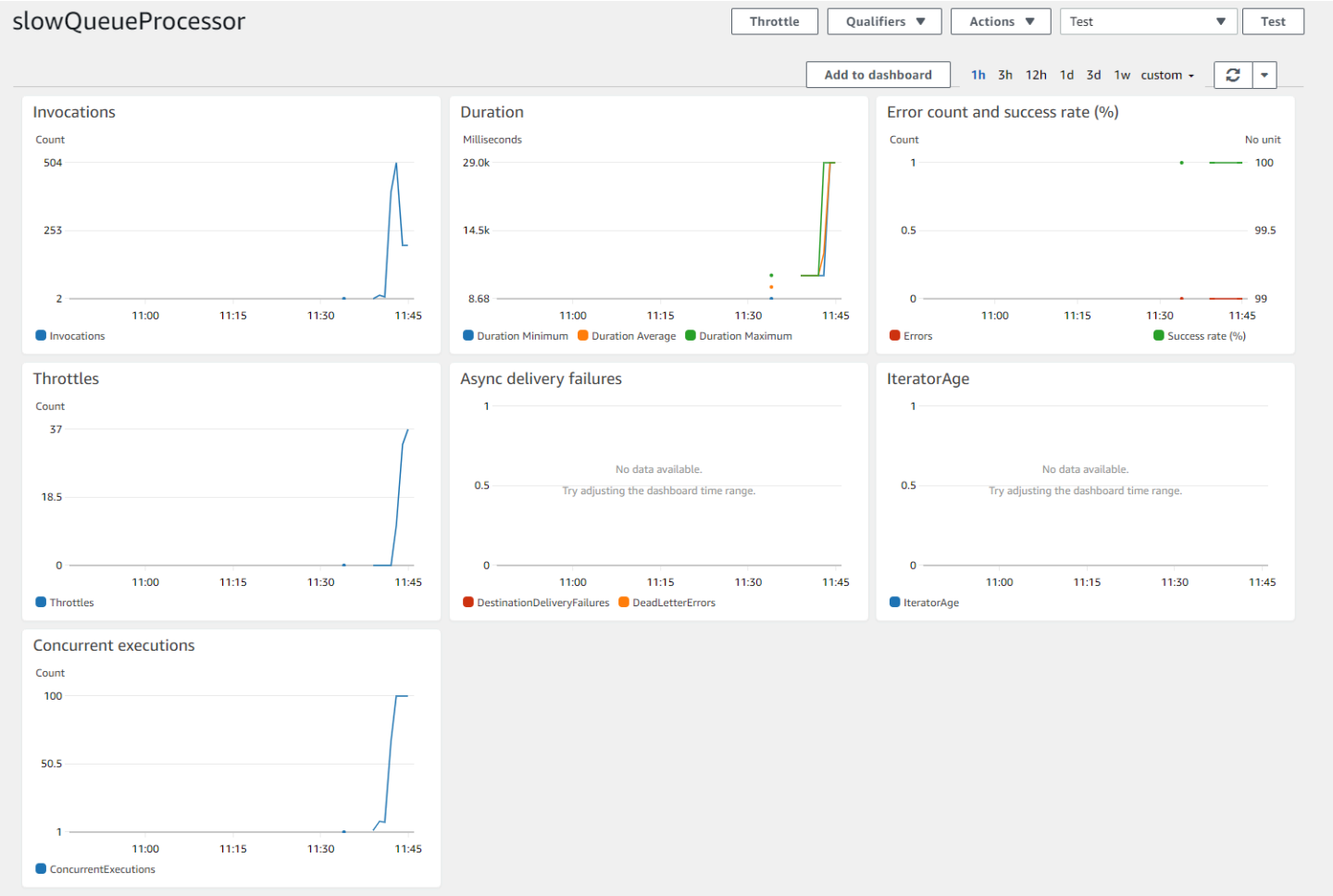
Identification et gestion de la limitation

Dans Lambda, la limitation se produit lorsque vous atteignez la limite de simultanéité de votre fonction ou de votre compte. Prenons l’exemple suivant, où une fonction Lambda lit les messages d’une file d’attente Amazon SQS. Cette fonction Lambda simule des appels de 30 secondes et a une taille de lot de 1. Cela signifie que la fonction ne traite qu’un seul message toutes les 30 secondes :

```
const doWork = (ms) => new Promise(resolve => setTimeout(resolve, ms))

exports.handler = async (event) => {
    await doWork(30000)
```

```
}
```

Avec une durée d'invocation aussi longue, les messages commencent à arriver dans la file d'attente plus rapidement qu'ils sont traités. Si la simultanéité non réservée de votre compte est de 100, Lambda augmente verticalement jusqu'à 100 exécutions simultanées, puis une limitation se produit. Vous pouvez voir ce schéma dans les CloudWatch métriques de la fonction :



CloudWatch les métriques de la fonction ne montrent aucune erreur, mais le graphique des exécutions simultanées indique que la simultanéité maximale de 100 est atteinte. Par conséquent, le graphique Limitations montre la limitation en place.

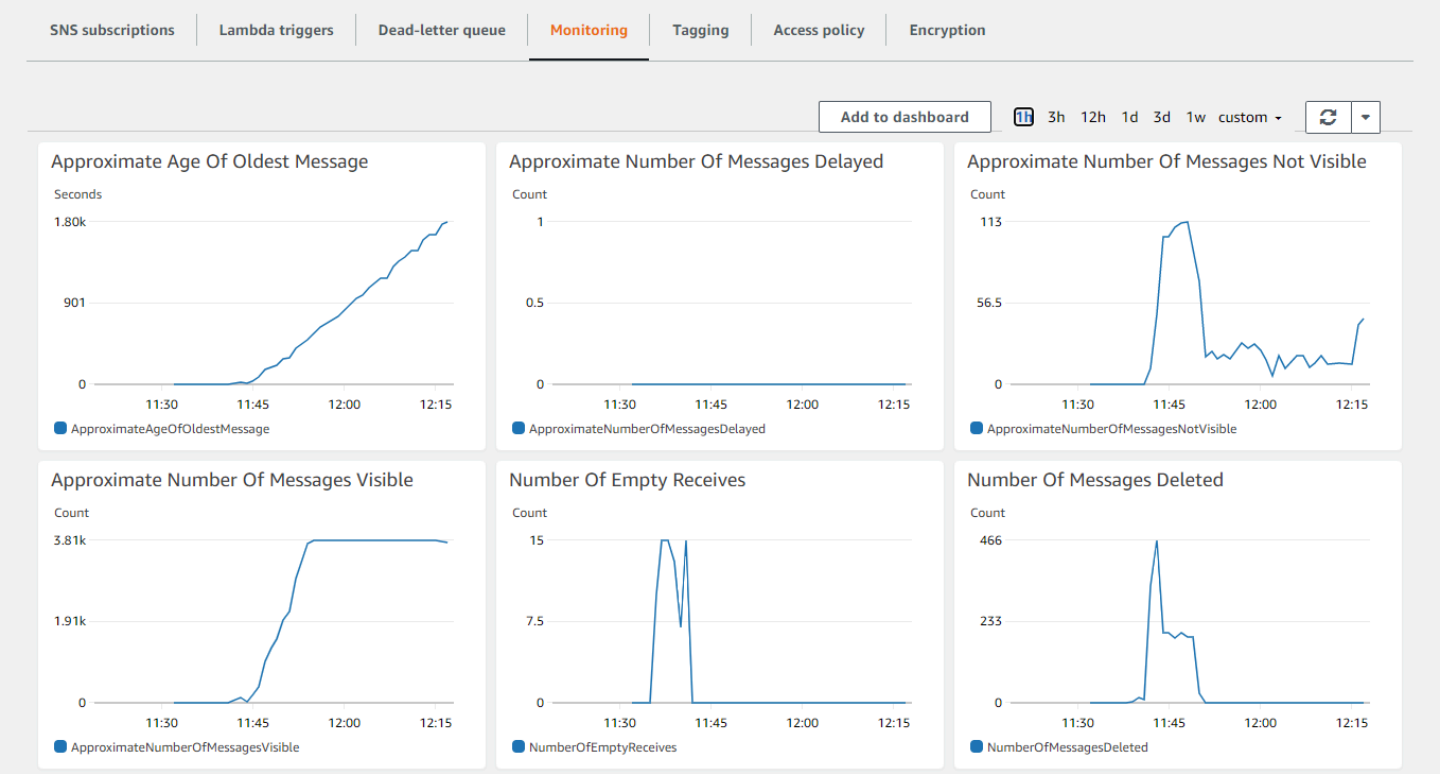
Vous pouvez détecter la régulation à l'aide d' CloudWatch alarmes et définir une alarme chaque fois que la métrique de régulation d'une fonction est supérieure à 0. Après avoir identifié le problème de limitation, plusieurs options s'offrent à vous pour le résoudre :

- Demandez une augmentation de la simultanéité auprès du AWS Support de cette région.

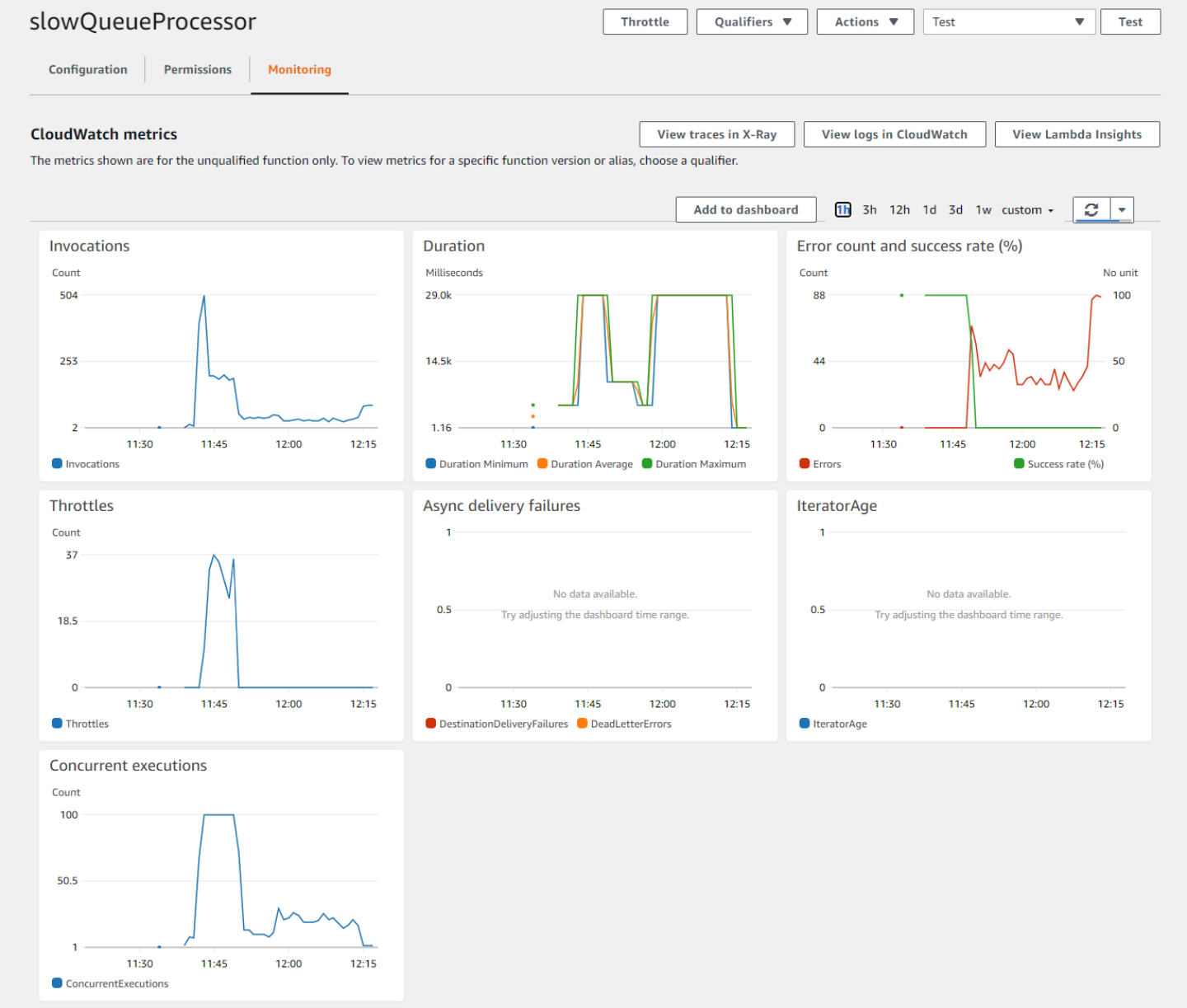
- Identifier les problèmes de performance de la fonction afin d'améliorer la vitesse de traitement et donc le débit.
- Augmenter la taille du lot de la fonction, de sorte que davantage de messages soient traités à chaque invocation.

Erreurs dans la fonction de traitement

Si la fonction de traitement génère des erreurs, Lambda renvoie les messages dans la file d'attente SQS. Lambda empêche la mise à l'échelle de votre fonction afin d'éviter les erreurs à grande échelle. Les métriques SQS suivantes CloudWatch indiquent un problème lié au traitement des files d'attente :

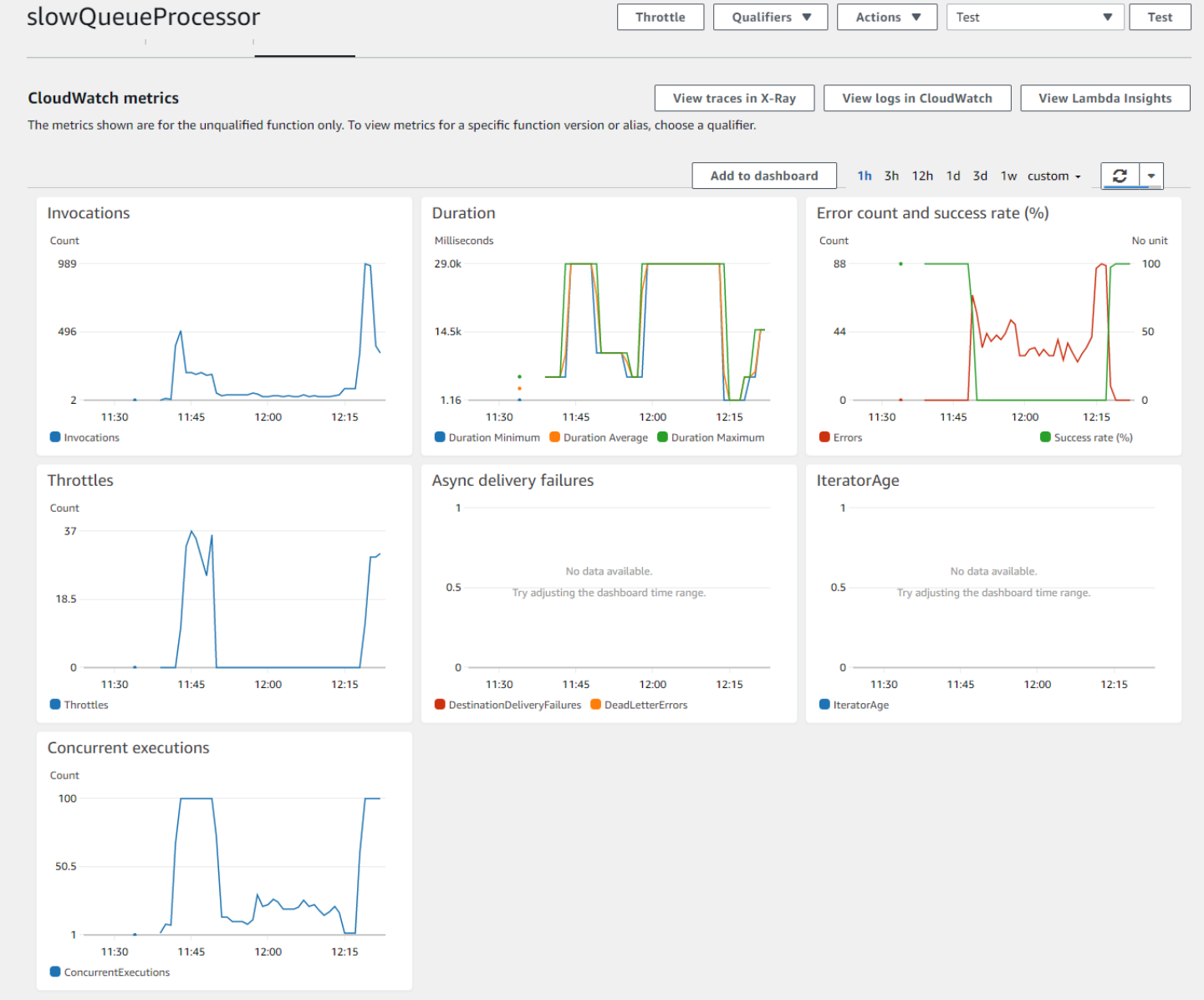


En particulier, l'âge du message le plus ancien et le nombre de messages visibles augmentent, alors qu'aucun message n'est supprimé. La file d'attente continue de croître, mais les messages ne sont pas traités. Les CloudWatch métriques de la fonction Lambda de traitement indiquent également l'existence d'un problème :



La métrique du Nombre d’erreurs est différente de zéro et augmente, tandis que les Exécutions simultanées ont diminué et que la limitation a cessé. Cela montre que Lambda a cessé de se mettre à l’échelle votre fonction en raison d’erreurs. Les CloudWatch journaux de la fonction fournissent des détails sur le type d'erreur.

Vous pouvez résoudre ce problème en identifiant la fonction à l’origine de l’erreur, puis en recherchant et en résolvant l’erreur. Une fois que vous avez corrigé l'erreur et déployé le nouveau code de fonction, les CloudWatch métriques devraient indiquer le processus de restauration :



Ici, la métrique Nombre d'erreurs tombe à zéro et la métrique Taux de réussite revient à 100 %. Lambda recommence à augmenter verticalement la fonction, comme indiqué dans le graphique Exécutions simultanées.

Identification et gestion de la contre-pression

Si un producteur d'événements génère régulièrement des messages pour une file d'attente SQS plus rapidement qu'une fonction Lambda peut le gérer, une contre-pression se produit. Dans ce cas, la surveillance SQS doit indiquer que l'âge du message le plus ancien augmente de façon linéaire, ainsi que le nombre approximatif de messages visibles. Vous pouvez détecter la contre-pression dans les files d'attente à l'aide CloudWatch d'alarmes.

Les étapes à suivre pour remédier à la contre-pression dépendent de votre charge de travail. Si l'objectif principal est d'augmenter la capacité de traitement et le débit par la fonction Lambda, plus options se présentent à vous :

- Demandez une augmentation via la console Service Quotas si votre fonction atteint le quota de simultanéité de votre compte.
- Activez le mode provisionné pour adapter le mappage des sources d'événements à une plus grande simultanéité. Pour plus d'informations, consultez Utilisation du mode provisionné avec les mappages de sources d'événements Amazon SQS.
- Augmenter la taille du lot de la fonction, de sorte que davantage de messages soient traités à chaque invocation.

Résolution des problèmes de réseaux dans Lambda

Par défaut, Lambda exécute vos fonctions dans un cloud privé virtuel (Virtual Private Cloud, VPC) interne disposant d'connectivité aux services AWS et à Internet. Pour accéder aux ressources réseau en local, vous pouvez configurer votre fonction afin qu'elle se connecte à un VPC de votre compte. Lorsque vous utilisez cette fonctionnalité, vous gérez l'accès Internet et la connectivité réseau de la fonction Lambda Event avec les ressources Amazon Virtual Private Cloud (Amazon VPC).

Les erreurs de connectivité réseau peuvent être dues à des problèmes liés à la configuration du routage de votre VPC, aux règles du groupe de sécurité, aux autorisations de rôle Gestion des identités et des accès AWS (IAM) ou à la traduction d'adresses réseau (NAT), ou à la disponibilité de ressources telles que les adresses IP ou les interfaces réseau. En fonction du problème, vous pouvez voir une erreur spécifique ou un délai d'attente si une requête ne peut pas atteindre sa destination.

Rubriques

- VPC : la fonction perd l'accès à Internet ou expire
- VPC : échec intermittent de la connexion TCP ou UDP
- VPC : la fonction doit avoir accès à Services AWS sans utiliser Internet
- VPC : limite d'interface réseau Elastic atteinte
- EC2 : interface réseau élastique de type « lambda »
- DNS : échec de la connexion aux hôtes avec UNKNOWNHOSTEXCEPTION

VPC : la fonction perd l'accès à Internet ou expire

Problème : votre fonction Lambda perd l'accès Internet après la connexion à un VPC.

Erreur : Error: connect ETIMEDOUT 176.32.98.189:443

Erreur : Error: Task timed out after 10.00 seconds

Erreur ReadTimeoutError : Le délai de lecture a expiré. (délai de lecture = 15)

Lorsque vous connectez une fonction à un VPC, toutes les demandes sortantes passent par le VPC. Pour vous connecter à Internet, configurez votre VPC pour envoyer le trafic sortant depuis le sous-réseau de la fonction vers une passerelle NAT dans un sous-réseau public. Pour obtenir plus d'informations et des exemples de configurations VPC, consultez the section called "Accès Internet pour les fonctions VPC".

Si certaines de vos connexions TCP sont interrompues, consultez the section called "VPC : échec intermittent de la connexion TCP ou UDP" si votre sous-réseau utilise une liste de contrôle d'accès (NACL). Dans le cas contraire, cela est probablement dû à la fragmentation des paquets. Les fonctions Lambda ne peuvent pas traiter les requêtes TCP fragmentées entrantes, car Lambda ne prend pas en charge la fragmentation IP pour TCP ou ICMP.

VPC : échec intermittent de la connexion TCP ou UDP

> **Note**
>
> Ce problème ne s'applique que si votre sous-réseau utilise une liste de contrôle d'accès (ACL) réseau. Les ACL réseau ne sont pas requises pour que Lambda se connecte à vos sous-réseaux.

Problème : Lambda perd par intermittence la connexion à vos sous-réseaux VPC, pour lesquels vous avez configuré une liste de contrôle d'accès (ACL) réseau.

Pour les fonctions VPC-enabled Lambda, AWS crée des ENI d'hyperplan dans le compte du client et utilise des ports éphémères pour `65535` connecter Lambda `1024` au VPC du client. Si vous utilisez des ACL réseau dans le sous-réseau cible, vous devez autoriser la plage de ports `1024` à `65535`, à la fois pour TCP et UDP. Ne pas autoriser cette plage complète de ports peut entraîner des défaillances de connexion intermittentes.

VPC : la fonction doit avoir accès à Services AWS sans utiliser Internet

Problème : Votre fonction Lambda doit être accessible Services AWS sans utiliser Internet.

Pour connecter une fonction Services AWS depuis un sous-réseau privé sans accès à Internet, utilisez des points de terminaison VPC.

VPC : limite d'interface réseau Elastic atteinte

Erreur ENILimitReachedException : La limite de l'interface Elastic network a été atteinte pour le VPC de la fonction.

Lorsque vous connectez une fonction Lambda à un VPC, Lambda crée une interface réseau Elastic pour chaque combinaison de sous-réseau et de groupe de sécurité attaché à cette fonction. Le quota de service par défaut est de 3 000 interfaces réseau par VPC. Pour demander une augmentation d'un quota, vous pouvez utiliser la console Service Quotas.

EC2 : interface réseau élastique de type « lambda »

Code d'erreur : Client.OperationNotPermitted

Message d'erreur : le groupe de sécurité ne peut pas être modifié pour ce type d'interface

Cette erreur s'affiche si vous tentez de modifier une Elastic Network Interface (ENI) gérée par Lambda. Le `ModifyNetworkInterfaceAttribute` n'est pas inclus dans l'API Lambda pour les opérations de mise à jour sur les interfaces réseau élastiques créées par Lambda.

DNS : échec de la connexion aux hôtes avec UNKNOWNHOSTEXCEPTION

Message d'erreur : UNKNOWNHOSTEXCEPTION

Les fonctions Lambda prennent en charge un maximum de 20 connexions TCP simultanées pour la résolution DNS. Votre fonction est peut-être en train d'épuiser cette limite. Les requêtes DNS les plus courantes sont effectuées via UDP. Si votre fonction établit uniquement des connexions DNS UDP, il est peu probable que ce soit votre problème. Cette erreur est souvent due à une mauvaise configuration ou à une infrastructure dégradée. Par conséquent, avant d'examiner votre trafic DNS en profondeur, vérifiez que votre infrastructure DNS est correctement configurée et saine et que votre fonction Lambda fait référence à un hôte spécifié dans le DNS.

Si vous diagnostiquez que votre problème est lié à la connexion TCP maximale, notez que vous ne pouvez pas demander d'augmentation de cette limite. Si votre fonction Lambda revient au DNS TCP

en raison de données utiles DNS importantes, vérifiez que votre solution utilise des bibliothèques compatibles EDNS. Pour plus d'informations sur l'extension EDNS, consultez la RFC 6891. Si vos charges utiles DNS dépassent régulièrement les tailles maximales EDNS, votre solution risque d'épuiser la limite DNS TCP.

Bonnes pratiques pour travailler avec AWS Lambda Fonctions événementielles

Les bonnes pratiques suivantes sont recommandées pour l'utilisation d' AWS Lambda :

Rubriques

- Code de fonction de l'événement
- Configuration de la fonction d'événement
- Extensibilité des fonctions événementielles
- Métriques et alarmes
- Utilisation des flux
- Bonnes pratiques de sécurité

Code de fonction de l'événement

Tirez parti de la réutilisation de l'environnement d'exécution pour améliorer les performances de votre fonction. Initialisez les clients SDK et les connexions à la base de données en dehors du gestionnaire de fonctions et mettez en cache les actifs statiques localement dans le répertoire `/tmp`. Les invocations ultérieures traitées par la même instance de votre fonction peuvent réutiliser ces ressources. Cela permet d'économiser des coûts, tout en réduisant le temps d'exécution de la fonction.

Pour éviter des éventuelles fuites de données entre les invocations, n'utilisez pas l'environnement d'exécution pour stocker des données utilisateur, des événements ou d'autres informations ayant un impact sur la sécurité. Si votre fonction repose sur un état réversible qui ne peut pas être stocké en mémoire dans le gestionnaire, envisagez de créer une fonction distincte ou des versions distinctes d'une fonction pour chaque utilisateur.

Utilisez une directive keep-alive pour maintenir les connexions persistantes. Lambda purge les connexions inactives au fil du temps. Si vous tentez de réutiliser une connexion inactive lorsque vous invoquez une fonction, cela entraîne une erreur de connexion. Pour maintenir votre connexion

persistante, utilisez la directive Keep-alive associée à votre environnement d'exécution. Pour un exemple, voir Réutilisation des connexions avec Keep-Alive in Node.js.

Utilisez des variables d'environnement pour transmettre des paramètres opérationnels à votre fonction. Par exemple, si vous écrivez dans un compartiment Amazon S3 au lieu de coder en dur le nom du compartiment dans lequel vous écrivez, configurez le nom du compartiment comme variable d'environnement.

Évitez d'utiliser des invocations récursives dans votre fonction Lambda, lorsque la fonction s'invoque elle-même ou démarre un processus susceptible de l'invoquer à nouveau. Cela peut entraîner un volume involontaire d'invocations de fonction et des coûts accrus. Si vous constatez un volume involontaire d'invocations, définissez immédiatement la simultanéité réservée à la fonction sur `0` afin de limiter toutes les invocations de la fonction, pendant que vous mettez à jour le code.

N'utilisez pas d'API non publiques non documentées dans le code de votre fonction Lambda. Pour les AWS Lambda environnements d'exécution gérés, Lambda applique régulièrement des mises à jour fonctionnelles et de sécurité aux API internes de Lambda. Ces mises à jour internes de l'API peuvent être incompatibles avec les versions antérieures, entraînant des conséquences imprévues telles que des échecs d'invocation si votre fonction dépend de ces API non publiques. Consultez la Référence d'API pour obtenir la liste des API accessibles au public.

Écriture du code idempotent. L'écriture de code idempotent pour vos fonctions garantit ne gestion identique des événements dupliqués. Votre code doit valider correctement les événements et gérer correctement les événements dupliqués. Pour de plus amples informations, veuillez consulterComment faire en sorte que ma fonction Lambda soit idempotente ?.

> **Note**
>
> Vous pouvez utiliser Powertools pour AWS Lambda rendre les fonctions idempotentes. Pour plus d'informations, consultez :
>
> - Python - Utilitaire d'idempotence
> - TypeScript - Utilitaire d'impuissance
> - Java - Utilitaire d'idempotence
> - .NET - Utilitaire d'idempotence

Pour connaître les pratiques exemplaires en matière de code spécifiques à chaque langage, reportez-vous aux sections suivantes :

- Meilleures pratiques en matière de code pour les Node.js fonctions d'événement Lambda
- Meilleures pratiques en matière de code pour les TypeScript fonctions d'événement Lambda
- Meilleures pratiques en matière de code pour les fonctions d'événement Lambda en Python
- Meilleures pratiques en matière de code pour les fonctions d'événement Ruby Lambda
- Meilleures pratiques en matière de code pour les fonctions d'événement Java Lambda
- Meilleures pratiques en matière de code pour les fonctions d'événement Go Lambda
- Meilleures pratiques en matière de code pour les fonctions d'événement Lambda en C#
- Bonnes pratiques en matière de code pour les fonctions d'événements Rust Lambda

Configuration de la fonction d'événement

Le test des performances de votre fonction d'événement Lambda est essentiel pour vous assurer de choisir la configuration de taille de mémoire optimale. Toute augmentation de la taille mémoire déclenche une augmentation équivalente de l'UC disponible pour votre fonction. L'utilisation de la mémoire pour votre fonction est déterminée par appel et peut être consultée sur Amazon CloudWatch. À chaque appel, une `REPORT:` entrée est effectuée, comme indiqué ci-dessous :

```
REPORT RequestId: 3604209a-e9a3-11e6-939a-754dd98c7be3 Duration: 12.34 ms Billed
 Duration: 100 ms Memory Size: 128 MB Max Memory Used: 18 MB
```

En analysant le champ `Max Memory Used:`, vous pouvez déterminer si votre fonction a besoin de plus de mémoire ou si vous avez surdimensionné la taille mémoire de votre fonction.

Pour trouver la configuration de mémoire adaptée à vos fonctions, nous vous recommandons d'utiliser le projet open source AWS Lambda Power Tuning. Pour plus d'informations, voir Réglage AWS Lambda de l'alimentation activé GitHub.

Pour optimiser les performances des fonctions, nous recommandons également de déployer des bibliothèques qui peuvent utiliser Advanced Vector Extensions 2 (AVX2). Vous pouvez ainsi traiter des charges de travail exigeantes, notamment l'inférence par apprentissage automatique, le traitement multimédia, le calcul haute performance (HPC), les simulations scientifiques et la modélisation financière. Pour plus d'informations, voir Création de AWS Lambda fonctions plus rapides avec AVX2.

Testez la charge de votre fonction d'événement Lambda pour déterminer une valeur de délai d'attente optimale. Il est important d'analyser la durée d'exécution de votre fonction afin de mieux

identifier tout problème lié à un service de dépendance susceptible d'augmenter la simultanéité de la fonction au-delà de vos attentes. Cela est particulièrement important lorsque votre fonction d'événement Lambda effectue des appels réseau vers des ressources susceptibles de ne pas gérer le dimensionnement de Lambda. Pour plus d'informations sur le test de charge de votre application, consultez Test de charge distribué sur AWS.

Utilisez les autorisations les plus restrictives lors de la définition des stratégies IAM. Comprenez les ressources et les opérations dont votre fonction d'événement Lambda a besoin, et limitez le rôle d'exécution à ces autorisations. Pour plus d'informations, consultez Gestion des autorisations dans AWS Lambda.

Familiarisez-vous avec Quotas Lambda. La taille de la charge utile, les descripteurs de fichiers et l'espace /tmp sont souvent ignorés lors de la détermination des limites des ressources.

Supprimez les fonctions d'événement Lambda que vous n'utilisez plus. En procédant ainsi, les fonctions inutilisées n'interviendront plus inutilement dans la limite de taille de votre package de déploiement.

Si vous utilisez Amazon Simple Queue Service en tant que source d'événement, assurez-vous que la valeur de la durée de l'invocation prévue de la fonction ne dépasse pas la valeur Délai de visibilité de la file d'attente. Cela s'applique à CreateFunction et UpdateFunctionConfiguration.

- Dans le cas de CreateFunction, le processus de création de la fonction AWS Lambda échoue.
- Dans le cas de UpdateFunctionConfiguration, cela pourrait entraîner des appels dupliqués de la fonction.

Extensibilité des fonctions événementielles

Familiarisez-vous avec vos contraintes de débit en amont et en aval. Bien que les fonctions d'événement Lambda s'adaptent parfaitement à la charge, les dépendances en amont et en aval peuvent ne pas avoir les mêmes capacités de débit. Si vous devez limiter le niveau de mise à l'échelle de votre fonction, configurez la simultanéité réservée sur votre fonction.

Créez une tolérance à la limitation. Si votre fonction synchrone est ralentie en raison d'un trafic dépassant le taux de mise à l'échelle de Lambda, vous pouvez utiliser les stratégies suivantes pour améliorer la tolérance à la limitation :

- Utilisez les délais d'expiration, les nouvelles tentatives et le backoff avec instabilité. La mise en œuvre de ces stratégies facilite les nouvelles tentatives d'invocation et permet de garantir

que Lambda peut se mettre à l'échelle en quelques secondes afin de minimiser la limitation des utilisateurs finaux.

- Utilisez la simultanéité allouée. La simultanéité allouée est le nombre d'environnements d'exécution préinitialisés que Lambda alloue à votre fonction. Lambda gère les requêtes entrantes en utilisant la simultanéité allouée lorsqu'elle est disponible. Lambda peut également mettre à l'échelle votre fonction au-delà de votre paramètre de simultanéité allouée si nécessaire. La configuration de la simultanéité provisionnée entraîne des frais supplémentaires pour votre compte. AWS

Métriques et alarmes

Utilisez Utilisation de CloudWatch métriques avec Lambda les CloudWatch alarmes et au lieu de créer ou de mettre à jour une métrique à partir de votre code de fonction d'événement Lambda. Il s'agit d'un moyen beaucoup plus efficace de suivre l'état de vos fonctions d'événement Lambda, ce qui vous permet de détecter les problèmes dès le début du processus de développement. Par exemple, vous pouvez configurer une alarme en fonction de la durée prévue de votre invocation de la fonction d'événement Lambda afin de remédier aux blocages ou aux latences attribuables à votre code de fonction.

Émettez des métriques personnalisées de manière asynchrone à l'aide du format EMF (Embedded Metric Format). Au lieu d'effectuer des appels d'API synchrones CloudWatch, utilisez EMF pour émettre des métriques via les journaux de votre fonction. Cette approche réduit la latence et améliore les performances.

L'utilitaire de métriques de Powertools pour AWS Lambda gère automatiquement le formatage EMF. Pour plus d'informations, consultez les utilitaires Python TypeScript, Java ou .NET Metrics dans la AWS Lambda documentation Powertools. Pour plus d'informations sur l'utilisation d'EMF pour générer des journaux au format métrique, consultez la section Publication de journaux avec le format métrique intégré dans le guide de l' CloudWatch utilisateur Amazon.

Utilisez la journalisation JSON structurée pour une meilleure observabilité. La journalisation structurée facilite la recherche, le filtrage et l'analyse des journaux de votre fonction. Envisagez d'utiliser l'utilitaire Logger de Powertools pour AWS Lambda formater automatiquement les journaux au format JSON. Pour plus d'informations, consultez les utilitaires Python TypeScript, Java ou .NET Logger dans la documentation Powertools. AWS Lambda

Utilisez votre bibliothèque de journalisation ainsi que AWS Lambda Metrics and Dimensions pour détecter les erreurs d'application (telles que ERR, ERROR et WARNING).

Utiliser Détection des anomalies de coûts AWS pour détecter les activités inhabituelles sur votre compte. La détection des anomalies de coûts utilise le machine learning pour effectuer une surveillance permanent de votre coût et votre utilisation, tout en minimisant les alertes de faux positifs. La détection des anomalies de coût utilise les données provenant de AWS Cost Explorer, avec un délai pouvant aller jusqu'à 24 heures.

Par conséquent, après utilisation, jusqu'à 24 heures peuvent être nécessaires pour détecter une anomalie. Afin de vous familiariser à la détection des anomalies de coûts, vous devez d'abord vous inscrire à Cost Explorer. Ensuite, accéder à la détection des anomalies des coûts.

Utilisation des flux

Testez différentes tailles de lot et d'enregistrement de telle sorte que la fréquence d'interrogation de chaque source d'événement soit réglée sur la vitesse à laquelle votre fonction peut exécuter sa tâche. Le CreateEventSourceMapping BatchSize paramètre contrôle le nombre maximum d'enregistrements pouvant être envoyés à votre fonction à chaque appel. Une taille de lot plus grande peut souvent absorber plus efficacement l'invocation sur un plus large ensemble d'enregistrements, ce qui accroît votre débit.

Par défaut, Lambda invoque votre fonction dès que des enregistrements sont disponibles. Si le lot que Lambda lit à partir de la source d'événements ne comprend qu'un seul enregistrement, Lambda envoie un seul registre à la fonction. Pour éviter d'invoquer la fonction avec un petit nombre de registres, vous pouvez indiquer à la source d'événement de les mettre en mémoire tampon pendant 5 minutes en configurant une fenêtre de traitement par lots. Avant d'invoquer la fonction, Lambda continue de lire les registres de la source d'événements jusqu'à ce qu'il ait rassemblé un lot complet, que la fenêtre de traitement par lot expire ou que le lot atteigne la limite de charge utile de 6 Mo. Pour plus d'informations, consultez Comportement de traitement par lots.

> **Warning**
>
> Les mappages des sources d'événements Lambda traitent chaque événement au moins une fois, et le traitement des enregistrements peut être dupliqué. Pour éviter les problèmes potentiels liés à des événements dupliqués, nous vous recommandons vivement de rendre votre code de fonction idempotent. Pour en savoir plus, consultez Comment rendre ma fonction Lambda idempotente dans le Knowledge Center. AWS

Activez la réponse partielle de lot pour le traitement des flux. Lorsque vous traitez des lots d'enregistrements provenant de flux comme Kinesis ou DynamoDB Streams, activez la réponse

partielle de lot pour permettre à Lambda de réessayer uniquement les enregistrements ayant échoué au lieu de réessayer le lot complet. Cela améliore l'efficacité du traitement et réduit les retraitements inutiles. Vous pouvez éventuellement utiliser l'utilitaire Batch de Powertools AWS Lambda pour simplifier les modèles de traitement par lots.

> **Note**
>
> Vous pouvez utiliser Powertools AWS Lambda pour le traitement par lots. Pour plus d'informations, consultez :
>
> - Python - Traitement par lots
> - TypeScript - Traitement par lots
> - Java - Traitement par lots
> - .NET – Traitement par lots

Augmentez le débit de traitement du flux Kinesis en ajoutant des partitions. Un flux Kinesis est composé d'une ou plusieurs partitions. La vitesse à laquelle Lambda peut lire les données de Kinesis s'échelonne linéairement en fonction du nombre de partitions.

L'augmentation du nombre de partitions augmente directement le nombre maximal d'invocations simultanées de la fonction d'événement Lambda et peut augmenter le débit de traitement de vos flux Kinesis. Pour de plus amples informations sur la relation entre les partitions et les invocations de fonctions, consultez the section called "Flux d'interrogation et de mise en lots". Si vous augmentez le nombre de partitions dans un flux Kinesis, assurez-vous d'avoir choisi une clé de partition appropriée (consultez Clés de partition) pour vos données, de façon à ce que les enregistrements associés se retrouvent sur les mêmes partitions et que vos données soient correctement distribuées.

Utilisez Amazon CloudWatch on IteratorAge pour déterminer si votre flux Kinesis est en cours de traitement. Par exemple, configurez une CloudWatch alarme avec un réglage maximal de 30 000 (30 secondes).

Bonnes pratiques de sécurité

Surveillez votre utilisation AWS Lambda en ce qui concerne les meilleures pratiques de sécurité en utilisant AWS Security Hub CSPM. Security Hub CSPM utilise des contrôles de sécurité pour évaluer les configurations des ressources et les normes de sécurité afin de vous aider à vous conformer aux différents cadres de conformité. Pour plus d'informations sur l'utilisation de Security Hub CSPM

pour évaluer les ressources Lambda, consultez la section AWS Lambda Contrôles du Guide de l'utilisateur. AWS Security Hub CSPM

Surveillez les journaux d'activité du réseau Lambda à l'aide d'Amazon Lambda Protection GuardDuty . GuardDuty La protection Lambda vous aide à identifier les menaces de sécurité potentielles lorsque les fonctions d'événement Lambda sont invoquées dans votre. Compte AWS Par exemple, si l'une de vos fonctions interroge une adresse IP associée à une activité liée aux cryptomonnaies. GuardDuty surveille les journaux d'activité réseau générés lorsqu'une fonction d'événement Lambda est invoquée. Pour en savoir plus, consultez la section Protection Lambda dans le guide de GuardDuty l'utilisateur Amazon.

Exemples d'applications Lambda

Le GitHub référentiel de ce guide inclut des exemples d'applications illustrant l'utilisation de différents langages et AWS services. Chaque exemple d'application comprend des scripts facilitant le déploiement et le nettoyage, ainsi que des ressources complémentaires.

Node.js

Exemples d'applications Lambda dans Node.js

- blank-nodejs — Node.js Fonction qui montre l'utilisation de la journalisation, des variables d'environnement, du AWS X-Ray traçage, des couches, des tests unitaires et du SDK. AWS
- nodejs-apig – Fonction avec un point de terminaison d'API public qui traite un événement d'API Gateway et renvoie une réponse HTTP.

Python

Exemples d'applications Lambda en Python

- blank-python — Fonction Python qui montre l'utilisation de la journalisation, des variables d'environnement, du AWS X-Ray traçage, des couches, des tests unitaires et du AWS SDK.

Ruby

Exemples d'applications Lambda en Ruby

- blank-ruby — Une fonction Ruby qui montre l'utilisation de la journalisation, des variables d'environnement, du AWS X-Ray traçage, des couches, des tests unitaires et du AWS SDK.

- Exemples de code Ruby pour AWS Lambda — Exemples de code écrits en Ruby qui montrent comment interagir avec Lambda AWS .

Java

Exemples d'applications Lambda en Java

- example-java — Une fonction d'événement Java qui montre comment utiliser Lambda pour traiter les commandes. Cette fonction montre comment définir et désérialiser un objet d'événement d'entrée personnalisé, utiliser le AWS SDK et enregistrer les sorties.
- java-basic – Ensemble de fonctions Java minimales avec des tests unitaires et une configuration de journalisation variable.
- java events – Ensemble de fonctions Java contenant du code squelette permettant de gérer les événements de divers services tels qu'Amazon API Gateway, Amazon SQS et Amazon Kinesis. Ces fonctions utilisent la dernière version (3.0.0 et ultérieure) de la bibliothèque aws-lambda-java-events. Ces exemples ne nécessitent pas le AWS SDK en tant que dépendance.
- s3-java – Fonction Java qui traite les événements de notification d'Amazon S3 et utilise la bibliothèque de classes Java (JCL) pour créer des miniatures à partir de fichiers d'image chargés.
- layer-java : fonction Java qui illustre comment utiliser une couche Lambda pour empaqueter les dépendances séparément du code de votre fonction principale.

Exécution de cadres Java populaires sur Lambda

- spring-cloud-function-samples — Exemple tiré de Spring qui montre comment utiliser le framework Spring Cloud Function pour créer des fonctions d'événement Lambda. AWS
- Démo de l'application Spring Boot sans serveur : exemple qui montre comment configurer une application Spring Boot typique dans un environnement d'exécution Java géré avec ou sans SnapStart, ou en tant qu'image native de GraalVM avec un environnement d'exécution personnalisé.
- Démonstration de l'application Micronaut sans serveur — Un exemple qui montre comment utiliser Micronaut dans un environnement d'exécution Java géré avec et sans SnapStart, ou en tant qu'image native de GraalVM avec un environnement d'exécution personnalisé. Pour en savoir plus, consultez les Micronaut/Lambda guides.
- Démo de l'application Quarkus sans serveur — Un exemple qui montre comment utiliser Quarkus dans un environnement d'exécution Java géré avec et sans SnapStart, ou en tant

qu'image native de GraalVM avec un environnement d'exécution personnalisé. Pour en savoir plus, consultez le Quarkus/Lambda guide et le Quarkus/SnapStart guide.

Go

Lambda fournit les exemples d'applications suivants pour l'environnement d'exécution Go :

Exemples d’applications Lambda en Go

- go-al2 – Une fonction Hello World qui renvoie l’adresse IP publique. Cette application utilise l’exécution personnalisée `provided.al2`.
- blank-go — Une fonction Go qui montre l'utilisation des bibliothèques Go de Lambda, de la journalisation, des variables d'environnement et du SDK. AWS Cette application utilise l'exécution `go1.x`.

C#

Exemples d'applications Lambda en C#

- blank-csharp – Fonction C# montrant l'utilisation des bibliothèques .NET de Lambda, la journalisation, les variables d'environnement, le suivi AWS X-Ray , les tests unitaires et le kit AWS SDK.
- blank-csharp-with-layer – Fonction C# qui utilise l'interface de ligne de commande .NET pour créer une couche permettant d'empaqueter les dépendances de la fonction.
- ec2-spot – Fonction qui gère les demandes d'instance Spot dans Amazon EC2.

PowerShell

Lambda fournit les exemples d'applications suivants pour : PowerShell

- blank-powershell — PowerShell Fonction qui montre l'utilisation de la journalisation, des variables d'environnement et du SDK. AWS

Pour déployer un exemple d'application, suivez les instructions de son fichier README.

Outils de développement pour Lambda

Vous avez accès à une variété d'outils qui augmentent la productivité et la facilité d'utilisation tout au long du cycle de développement. Cette section propose des informations sur des outils qui aident de nombreux clients Lambda à concevoir, développer et gérer leurs applications. Du développement local dans votre IDE au déploiement et à la gestion d'applications sans serveur complexes, ces outils vous aident à rationaliser votre flux de travail, à améliorer la qualité du code et à accélérer le développement de Lambda-based solutions robustes.

- Développement local — Écrivez et testez les fonctions d'événement Lambda plus rapidement dans votre environnement de développement préféré. Le AWS Toolkit for VS Code permet le développement, le débogage et le test de fonctions locales avec des fonctionnalités de déploiement direct sur Lambda.
- Infrastructure en tant que code (IaC) : déployez et gérez les applications sans serveur de manière cohérente, des tests locaux à la production. AWS SAM AWS CDK, et CloudFormation vous permet de définir et de gérer votre infrastructure sans serveur via du code pour des déploiements cohérents et contrôlés par version.
- GitHub Actions — Automatisez les déploiements Lambda directement depuis votre référentiel de code. Avec GitHub Actions, vous pouvez configurer des flux de travail qui déploient automatiquement vos fonctions Lambda chaque fois que vous modifiez le code ou la configuration, simplifiant ainsi votre pipeline. CI/CD
- Powertools for AWS Lambda : créez des applications sans serveur prêtes pour la production avec moins de code personnalisé. Powertools for AWS Lambda (également appelé Powertools AWS for) est une boîte à outils de développement open source qui simplifie la mise en œuvre des meilleures pratiques sans serveur telles que l'observabilité, la récupération de paramètres et l'idempotentie en Python, Java et .NET. TypeScript
- Flux de travail et événements : coordonnez les fonctions Lambda avec les AWS services, les API et les systèmes externes. Lambda propose deux options d'orchestration : des fonctions durables Lambda pour une orchestration centrée sur les applications à l'aide de langages de programmation standard au sein de Lambda, AWS Step Functionset pour une orchestration centrée sur le flux de travail avec une conception visuelle pour plusieurs services. Amazon EventBridge fournit des fonctionnalités de gestion des événements pour les architectures axées sur les événements. Pour obtenir de l'aide sur le choix d'une approche d'orchestration, consultez Durable functions ou Step Functions.

Outils de développement locaux

Les environnements de développement locaux vous permettent de travailler hors ligne et d'utiliser les fonctionnalités avancées de l'IDE tout en itérant rapidement sur vos fonctions Lambda. Ces outils vous aident à déboguer les fonctions complexes et à les développer dans des environnements où la connectivité est limitée. Ils favorisent également la collaboration en équipe et l'intégration avec les systèmes de contrôle de version.

Pour plus d'informations sur le développement de fonctions Lambda localement, consultez Développement de fonctions événementielles localement. Cette page explique comment déplacer le développement de fonctions Lambda de la AWS console vers Visual Studio Code, qui fournit un environnement de développement riche avec des fonctionnalités telles que le débogage et la complétion du code. Pour effectuer la transition, vous devez configurer les informations d'identification AWS Toolkit for Visual Studio Code et, après quoi vous pourrez utiliser les fonctionnalités avancées de VS Code tout en conservant la possibilité de déployer directement vers AWS.

Le développement local pour Lambda offre plusieurs fonctionnalités clés :

- Utiliser l'intégration de Visual Studio Code avec la console Lambda
- Configurer des environnements de développement Lambda locaux
- Déboguer et tester les fonctions localement
- Appliquer les bonnes pratiques de gestion des fonctions locales

Pour plus d'informations, consultez Développement de fonctions événementielles localement.

Outils d'infrastructure en tant que code (IaC)

Avec les outils d'infrastructure en tant que code (IaC), vous pouvez définir et gérer votre architecture sans serveur à l'aide de code. Cette approche permet de maintenir la cohérence entre les environnements, vous permet de contrôler les versions de votre infrastructure et soutient les DevOps pratiques. L'IaC est particulièrement utile pour automatiser les déploiements, garantir la cohérence des environnements et gérer les déploiements multirégionaux.

Les principaux outils et concepts IaC pour Lambda incluent des cadres pour la création de modèles, la gestion du déploiement et des bonnes pratiques pour l'infrastructure sans serveur :

- Principes fondamentaux de l'IaC pour le développement Lambda

- CloudFormation AWS SAM, et AWS CDK fonctionnalités
- Critères de sélection et comparaison des outils
- Bonnes pratiques de mise en œuvre l'IaC Lambda

Que vous travailliez de manière indépendante sur un petit projet ou que vous fassiez partie d'une grande équipe gérant des applications sans serveur à l'échelle de l'entreprise, ces outils de développement et de déploiement peuvent vous aider à écrire, déployer et gérer vos fonctions Lambda de manière plus efficace.

Pour plus d'informations, consultez Utilisation de Lambda avec infrastructure en tant que code (IaC).

GitHub Outils d'actions

GitHub Actions fournit des fonctionnalités de déploiement automatique pour vos fonctions Lambda directement à partir de votre référentiel de code. En créant des fichiers de flux de travail dans votre référentiel, vous pouvez déployer automatiquement les fonctions Lambda chaque fois que des modifications de code ou de configuration sont apportées, rationalisant ainsi votre pipeline d'intégration continue et de déploiement continu ()CI/CD. L'action de la fonction Deploy Lambda propose une interface YAML déclarative qui simplifie le processus de déploiement, gère les informations d'identification via AWS OpenID Connect (OIDC) et prend en charge divers scénarios de déploiement, notamment les mises à jour du code, les modifications de configuration et les validations à sec. Cette intégration permet aux équipes de maintenir un processus de déploiement cohérent et automatisé tout en utilisant leurs GitHub flux de travail existants.

Pour plus d'informations, consultez Utilisation d' GitHub actions pour déployer des fonctions d'événement.

Outils électriques pour AWS Lambda

Powertools for AWS est une boîte à outils de développement open source qui vous aide à mettre en œuvre les meilleures pratiques sans serveur avec un minimum de code personnalisé. Disponible pour Python, Java et .NET TypeScript/Node.js, il fournit des fonctions utilitaires, des décorateurs et des intergiciels qui rationalisent les tâches de développement Lambda courantes. La boîte à outils inclut des fonctionnalités d'observabilité intégrées comme la journalisation structurée, le suivi et la collecte de métriques, notamment avec des utilitaires pour la récupération des paramètres, la gestion des secrets et des modèles d'idempotence. Ces outils s'alignent sur les meilleures pratiques AWS bien conçues et aident les développeurs à créer plus efficacement des applications sans serveur prêtes pour la production. En réduisant le code standard et en normalisant les modèles courants,

Powertools for AWS permet aux équipes de se concentrer sur la logique métier tout en maintenant une mise en œuvre cohérente des meilleures pratiques sans serveur dans leurs applications.

Pour plus d'informations, consultez Outils électriques pour AWS Lambda.

Outils de gestion des flux de travail et des événements

Les applications Lambda peuvent être utilisées pour l'orchestration de flux de travail complexes et la gestion de divers événements. AWS fournit des outils spécialisés pour vous aider à gérer ces aspects du développement sans serveur. Découvrez l'orchestration AWS Step Functions des flux de travail et Amazon EventBridge pour la gestion des événements, ainsi que la manière de les intégrer à vos fonctions Lambda. Ces outils peuvent améliorer de manière significative la capacité de mise à l'échelle et la fiabilité de vos applications sans serveur en fournissant une gestion d'état robuste et des architectures pilotées par les événements. En utilisant ces services, vous pouvez créer des Lambda-based solutions plus sophistiquées et résilientes capables de gérer des processus métier complexes et de réagir à un large éventail d'événements liés au système et aux applications.

Pour plus d'informations, consultez Gestion des flux de travail et des événements Lambda.

Développement de fonctions événementielles localement

Vous pouvez déplacer vos fonctions d'événement Lambda de la console Lambda vers votre environnement de développement intégré (IDE) préféré, qui fournit un environnement de développement complet dans lequel vous pouvez utiliser d'autres options de développement locales telles que et. AWS SAM AWS CDK La console Lambda prend en charge l'ouverture de fonctions directement dans Visual Studio Code, Kiro ou Cursor.

Principaux avantages du développement local

Bien que la console Lambda permette de modifier et de tester rapidement des fonctions, le développement local offre des fonctionnalités plus avancées :

- Fonctionnalités avancées de l'IDE : outils de débogage, de complétion de code et de refactorisation
- Développement hors ligne : travaillez et testez les modifications localement avant de les déployer dans le cloud
- Intégration de l'infrastructure en tant que code : utilisation fluide avec AWS SAM et Infrastructure Composer AWS CDK
- Gestion des dépendances : contrôle total sur les dépendances des fonctions

Conditions préalables

Avant de développer des fonctions Lambda localement à l'aide de Visual Studio Code, Kiro et Cursor, vous devez les installer en suivant les instructions ci-dessous :

- Visual Studio Code : pour les instructions d'installation, voir Télécharger Visual Studio Code.
- Kiro : pour les instructions d'installation, voir Commencer à utiliser Kiro.
- Curseur : pour les instructions d'installation, voir Télécharger le curseur.

Vous avez également besoin des éléments suivants :

- AWS Toolkit for Visual Studio Code: pour les instructions d'installation de Visual Studio Code, voir Configuration du AWS Toolkit for Visual Studio Code. Pour avoir une présentation, consultez AWS Toolkit for Visual Studio Code.
- AWS informations d'identification : pour plus d'informations sur la configuration des informations d'identification, voir Configuration de vos AWS informations d'identification.
- AWS SAMCLI: Pour les instructions d'installation, reportez-vous à la section Installation du AWS SAMCLI.
- Docker installé (facultatif, mais obligatoire pour les tests locaux) : pour les instructions d'installation, consultez Obtenir Docker.

> **Note**
>
> Si vous avez déjà configuré un AWS compte et un profil localement, assurez-vous que la politique AdministratorAccess gérée est ajoutée à votre AWS profil configuré.

Authentification et contrôle d'accès

Pour développer des fonctions Lambda localement, vous avez besoin AWS d'informations d'identification pour accéder aux AWS ressources en toute sécurité et les gérer en votre nom, comme elles le feraient dans le cloud.

Le AWS Toolkit for Visual Studio Code prend en charge les méthodes d'authentification suivantes :

- Informations d'identification à long terme des utilisateurs IAM
- Informations d'identification temporaires de rôles assumés

- Fédération des identités
- AWS informations d'identification de l'utilisateur root du compte (non recommandé)

Cette section vous explique comment obtenir et configurer ces informations d’identification à l’aide des informations d’identification à long terme d’utilisateur IAM.

Obtenir les informations d’identification IAM

Si un utilisateur IAM possède déjà des clés d’accès, préparez l’ID de clé d’accès et la clé d’accès secrète pour la section suivante. Si vous ne possédez pas ces clés, suivez ces étapes pour les créer :

> **Note**
>
> Vous devez utiliser à la fois l'ID de la clé d'accès et la clé d'accès secrète pour authentifier vos demandes.

Pour créer un utilisateur IAM et des clés d’accès :

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/
2. Dans le panneau de navigation, sélectionnez Users.
3. Choisissez Create user (Créer un utilisateur).
4. Dans Nom d’utilisateur, entrez un nom et choisissez Suivant.
5. Pour Set permissions (Définir les autorisations), sélectionnez Attacher directement les stratégies.
6. Sélectionnez AdministratorAccesset choisissez Next.
7. Choisissez Create user (Créer un utilisateur).
8. Dans la bannière indiquant le succès, choisissez Voir l’utilisateur.
9. Choisissez Create access key (Créer une clé d’accès).
10. Pour Cas d’utilisation, sélectionnez Code local.
11. Cochez la case de confirmation et choisissez Suivant.
12. (Facultatif) Entrez une valeur de balise de description.
13. Choisissez Create access key (Créer une clé d’accès).
14. Copiez immédiatement votre clé d’accès et votre clé d’accès secrète. Vous ne pourrez plus accéder à la clé d’accès secrète après avoir quitté cette page.

> **Important**
>
> Ne partagez jamais votre clé secrète et ne la confiez jamais au contrôle de source. Stockez ces clés en toute sécurité et supprimez-les lorsqu'elles ne sont plus nécessaires.

> **Note**
>
> Pour plus d'informations, consultez les sections Créer un utilisateur IAM dans votre AWS compte et Gérer les clés d'accès pour les utilisateurs IAM dans le guide de l'utilisateur IAM.

Configurer AWS informations d'identification à l'aide du AWS Boîte à outils

Le tableau suivant récapitule le processus de configuration des informations d'identification que vous avez effectué dans le cadre de la procédure suivante.

Que faire	Pourquoi ?
Ouvrez le panneau Connexion	Démarrer l'authentification
Utilisez la palette de commandes, recherchez AWS Ajouter une nouvelle connexion	Accédez à l'interface de connexion
Choisissez Informations d'identification IAM	Utiliser vos clés d'accès pour l'accès programmatique
Saisissez le nom du profil, la clé d'accès et la clé secrète	Fournir les informations d'identification pour la connexion
Voir la mise à jour de AWS Explorer	Confirmez que vous êtes connecté

Procédez comme suit pour vous authentifier auprès de votre AWS compte :

> **Note**
>
> Les étapes suivantes s'appliquent à Visual Studio Code, Kiro et Cursor. Kiro et Cursor étant basés sur Visual Studio Code, le flux d'authentification est le même dans les trois IDE.

1. Ouvrez le panneau de connexion dans votre IDE :

   Pour démarrer le processus d'authentification, sélectionnez l' AWS icône dans le volet de navigation de gauche ou ouvrez la palette de commandes (Cmd+Shift+P sur Mac ou Ctrl+Shift+P activé Windows/Linux), recherchez et sélectionnez Ajouter une nouvelle connexion.AWS
2. Dans le panneau de connexion, choisissez Informations d'identification IAM, puis sélectionnez Continuer.

   > **Note**
   >
   > Pour continuer, vous devez autoriser les extensions AWS IDE à accéder à vos données.
3. Saisissez le nom de votre profil, l'ID de clé d'accès et la clé d'accès secrète, puis sélectionnez Continuer.
4. Vérifiez la connexion en vérifiant la présence de vos AWS services et ressources dans l' AWS explorateur de votre IDE.

Pour plus d'informations sur la configuration de l'authentification avec des informations d'identification à long terme, voir Utilisation d'informations d'identification à long terme pour authentifier AWS les SDK et les outils.

Pour plus d'informations sur la configuration de l'authentification, consultez les informations d'identification AWS IAM dans le guide de AWS Toolkit for Visual Studio Code l'utilisateur.

Déplacement de la console au développement local

> **Note**
>
> Si vous avez apporté des modifications à la console, assurez-vous qu'il n'y a aucune modification non déployée avant de passer au développement local.

Pour déplacer une fonction Lambda de la console Lambda vers un IDE local, procédez comme suit :

1. Ouvrez la console Lambda.
2. Choisissez le nom de votre fonction .
3. Sélectionnez l'onglet Source du code.

4. Ouvrez votre fonction dans l'IDE de votre choix en cliquant sur la flèche déroulante à côté du bouton. Les options prises en charge sont Ouvrir dans Visual Studio Code, Ouvrir dans Kiro et Ouvrir dans le curseur.

   > **Note**
   >
   > Votre sélection IDE est conservée. Une fois que vous avez choisi un IDE, les visites suivantes indiquent cet IDE comme bouton principal.

5. Lorsque vous y êtes invité, autorisez votre navigateur à ouvrir l'IDE sélectionné.

Lorsque vous ouvrez votre fonction dans votre IDE, Lambda crée un projet local avec votre code de fonction dans un emplacement temporaire conçu pour des tests et un déploiement rapides. Cela inclut le code de fonction, les dépendances et une structure de projet de base que vous pouvez utiliser pour le développement local.

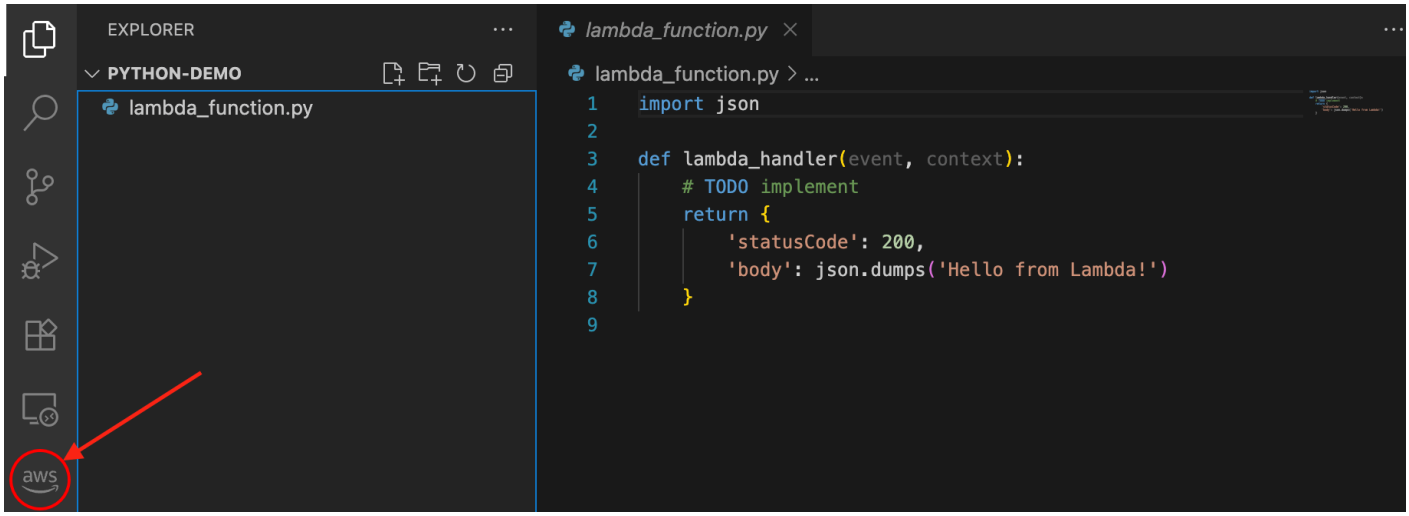
> **Note**
>
> Le bouton Ouvrir dans l'IDE nécessite la version 3.69.0 ou ultérieure du AWS Toolkit. Si une version antérieure du AWS Toolkit est installée, un `Cannot open the handler` message peut s'afficher. Pour résoudre ce problème, mettez à jour votre AWS boîte à outils avec la dernière version.

Pour plus de détails sur l'utilisation AWS dans votre IDE, consultez le guide de AWS Toolkit for Visual Studio Code l'utilisateur.

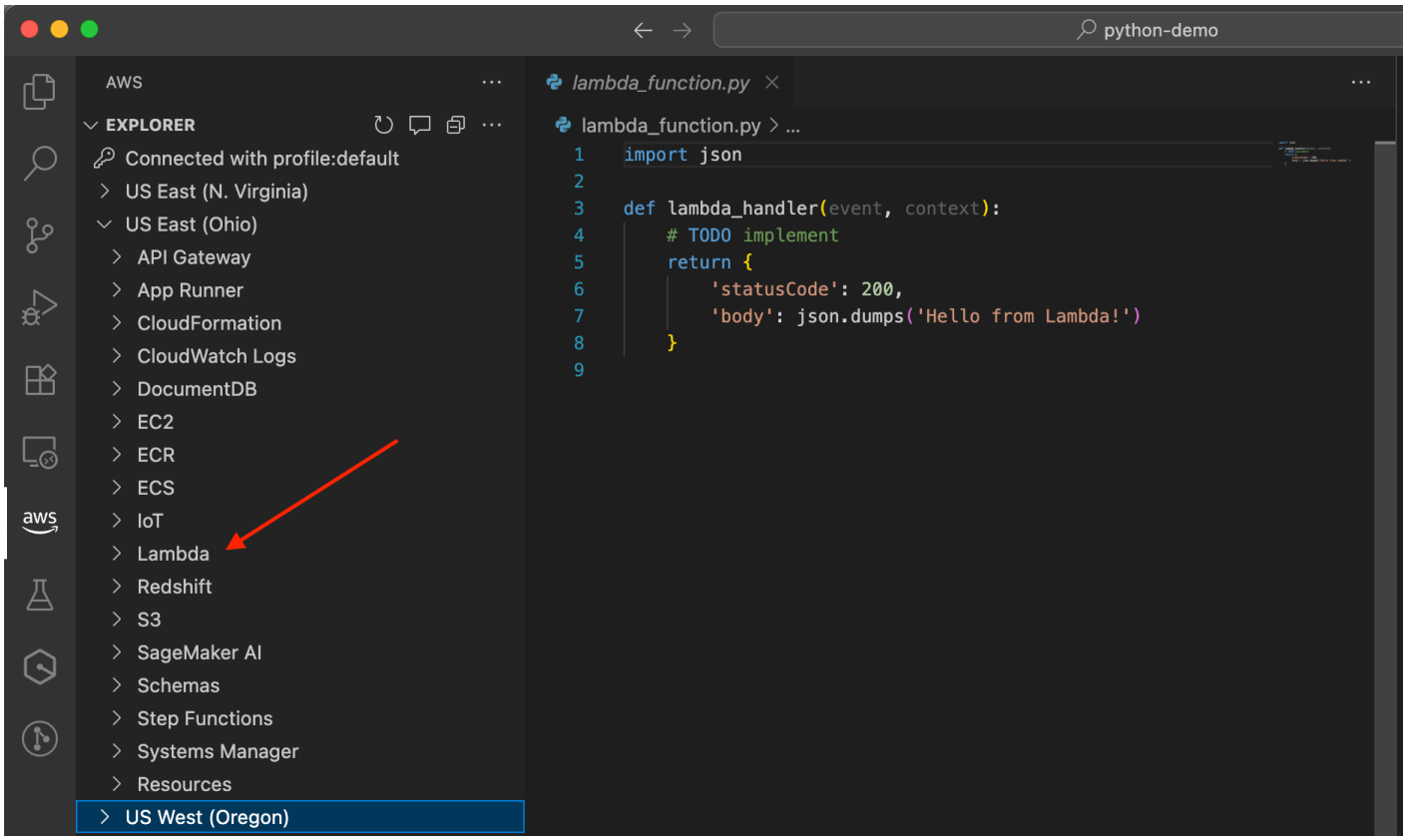
Utilisation des fonctions localement

Après avoir ouvert votre fonction dans votre IDE préféré, suivez ces étapes pour accéder à vos fonctions et les gérer. Pour l'exemple ci-dessous, nous avons utilisé Visual Studio Code.

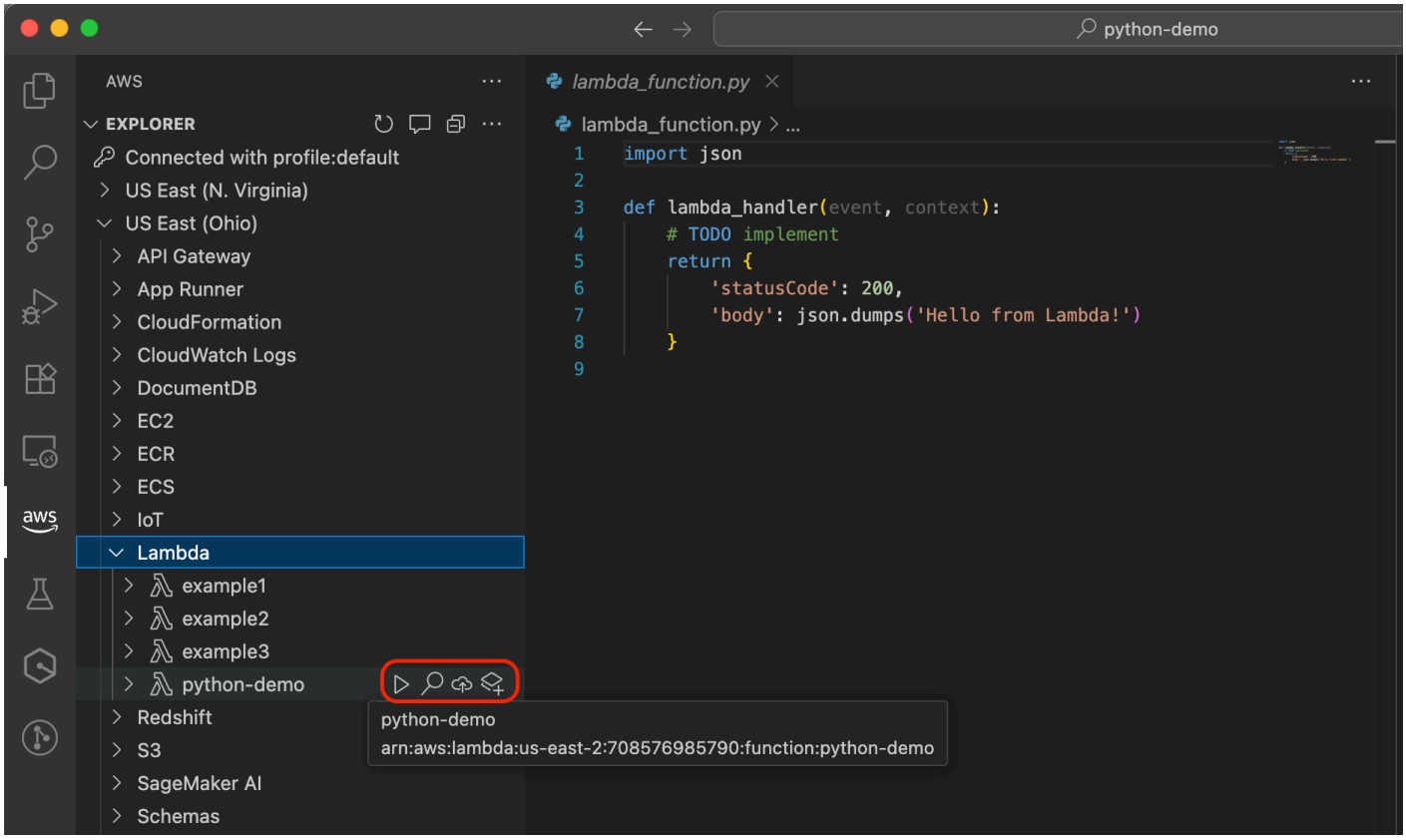
1. Sélectionnez l' AWS icône dans la barre latérale pour ouvrir l' AWS explorateur :



2. Dans l' AWS explorateur, sélectionnez la région dans laquelle se trouve votre fonction Lambda :



3. Dans la région que vous avez sélectionnée, développez la section Lambda pour voir et gérer vos fonctions :



Une fois votre fonction ouverte dans votre IDE, vous pouvez :

- Modifier le code de fonction avec prise en charge complète du langage et saisie semi-automatique du code.
- Utilisez l'LocalStack intégration pour tester les fonctions Lambda qui envoient des appels d'API à d'autres personnes Services AWS pendant l'exécution, par exemple en lisant des tables DynamoDB ou en écrivant dans des compartiments Amazon S3. LocalStack est un émulateur de services cloud qui fournit un environnement de développement local complet pour tester les intégrations de services. Vous pouvez également utiliser AWS SAM CLI pour tester votre fonction dans un conteneur local. Si votre fonction fait des appels d'API à d'autres Services AWS, ces appels atteindront AWS des ressources réelles, et non des ressources émulées.
- Déboguez votre fonction avec des points d'arrêt et l'inspection des variables. Pour plus d'informations, consultez Exécution et débogage de fonctions Lambda directement à partir du code dans le Guide de l'utilisateur AWS Toolkit for Visual Studio Code .
- Déployez à nouveau votre fonction mise à jour AWS en utilisant l'icône du cloud.
- Installez et gérez les dépendances de votre fonction.

Convertissez votre fonction en AWS SAM modéliser et utiliser les outils IaC

Dans tous les IDE compatibles (Visual Studio Code, Kiro et Cursor), vous pouvez convertir votre fonction Lambda en modèle en choisissant l'icône Convertir en application AWS SAM à côté de votre fonction Lambda. AWS SAM Vous êtes invité à sélectionner l'emplacement AWS SAM du projet. Une fois sélectionnée, votre fonction Lambda est convertie en un `template.yaml` fichier qui est enregistré dans votre nouveau AWS SAM projet.

Une fois votre fonction convertie en AWS SAM modèle, vous pouvez :

- Contrôler la gestion des versions de votre infrastructure
- Automatiser les déploiements
- Déboguer les fonctions à distance
- Ajoutez des AWS ressources supplémentaires à votre application
- Maintenir des environnements cohérents tout au long de votre cycle de développement
- Utilisez Infrastructure Composer pour modifier visuellement votre AWS SAM modèle

Pour plus d’informations sur l’utilisation des outils IaC, consultez les guides suivants :

- Le guide AWS Serverless Application Model du développeur
- Le guide Cloud Development Kit AWS (AWS CDK) du développeur
- Guide du développeur Infrastructure Composer
- Le guide de AWS CloudFormation l'utilisateur

Ces outils fournissent des fonctionnalités supplémentaires pour définir, tester et déployer vos applications sans serveur.

Étapes suivantes

Pour en savoir plus sur l'utilisation des fonctions Lambda dans Visual Studio Code, consultez les ressources suivantes :

- Utilisation des fonctions AWS Lambda dans le AWS guide de l'utilisateur du code Toolkit for Visual Studio
- Utilisation d'applications sans serveur dans le AWS guide de l'utilisateur du Toolkit for Visual Studio Code

- Infrastructure en tant que code dans le Guide du développeur Lambda

Utilisation d' GitHub actions pour déployer des fonctions d'événement

Vous pouvez utiliser GitHub les actions pour déployer automatiquement les fonctions d'événement Lambda lorsque vous envoyez des modifications de code ou de configuration à votre référentiel. L'action Déployer la fonction Lambda fournit une interface YAML simple et déclarative qui élimine la complexité des étapes de déploiement manuelles.

Exemple de flux de travail

Pour configurer le déploiement automatique des fonctions Lambda, créez un fichier de flux de travail dans le répertoire `.github/workflows/` de votre référentiel :

Example GitHub Flux de travail d'actions pour le déploiement de Lambda

```
name: Deploy AWS Lambda
on:
  push:
    branches:
      - main

jobs:
  deploy:
    runs-on: ubuntu-latest
    permissions:
      id-token: write # Required for OIDC authentication
      contents: read  # Required to check out the repository
    steps:
      - uses: actions/checkout@v4

      - name: Configure AWS credentials
        uses: aws-actions/configure-aws-credentials@v4
        with:
          role-to-assume: arn:aws:iam::123456789012:role/GitHubActionRole
          aws-region: us-east-1

      - name: Deploy Lambda Function
        uses: aws-actions/aws-lambda-deploy@v1
        with:
          function-name: my-lambda-function
```

```
          code-artifacts-dir: ./dist
```

Ce flux de travail s'exécute lorsque vous apportez des modifications à la branche `main`. Il vérifie votre dépôt, configure les AWS informations d'identification à l'aide d'OpenID Connect (OIDC) et déploie votre fonction à l'aide du code du répertoire. `./dist`

Pour d'autres exemples, notamment la mise à jour de la configuration des fonctions, le déploiement via des compartiments S3 et la validation de l'exécution à sec, consultez le fichier README de la fonction Deploy Lambda.

Ressources supplémentaires

- GitHub Action de configuration AWS des informations d'identification
- Configuration d'OpenID Connect dans AWS

Utilisation de Lambda avec infrastructure en tant que code (IaC)

Les fonctions d'événement Lambda s'exécutent rarement de manière isolée. Elles font souvent partie d'une application sans serveur avec d'autres ressources telles que les bases de données, les files d'attente et le stockage. Grâce à l'infrastructure sous forme de code (IaC), vous pouvez automatiser vos processus de déploiement afin de déployer et de mettre à jour rapidement et de manière répétée des applications sans serveur complètes impliquant de nombreuses ressources distinctes. AWS Cette approche accélère votre cycle de développement, facilite la gestion des configurations et garantit que vos ressources sont déployées de la même manière à chaque fois.

Outils de l'IaC pour Lambda

CloudFormation

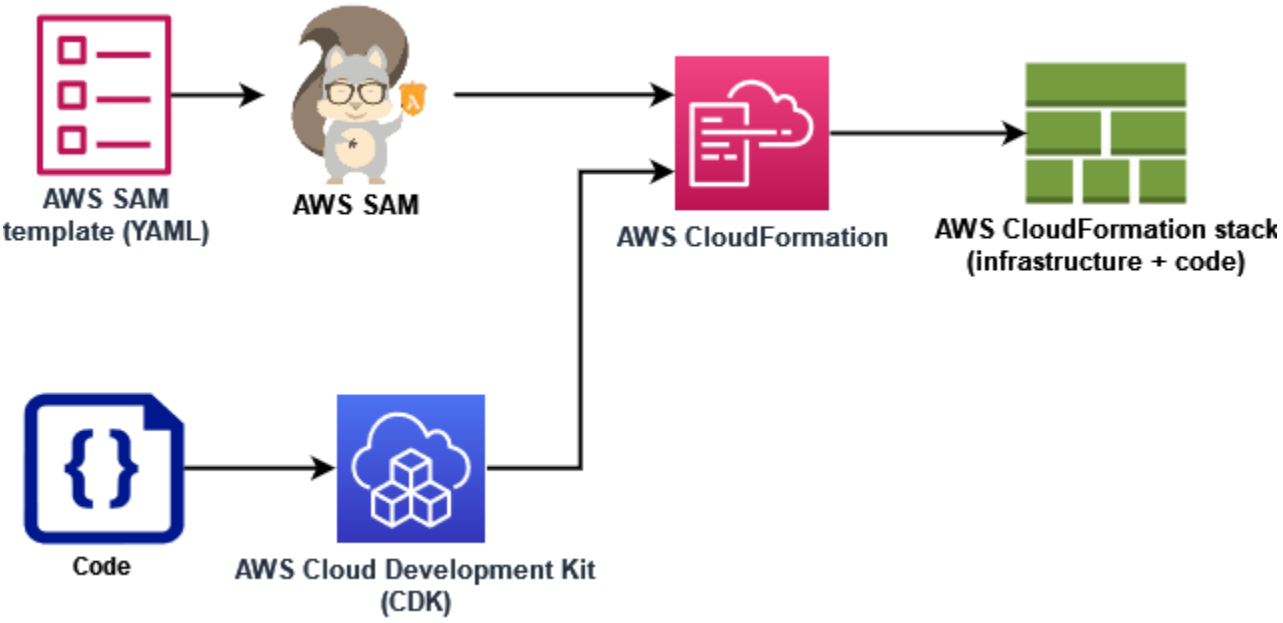
CloudFormation est le service IaC de base de AWS. Vous pouvez utiliser des modèles YAML ou JSON pour modéliser et provisionner l'ensemble de votre AWS infrastructure, y compris les fonctions Lambda. CloudFormation gère les complexités liées à la création, à la mise à jour et à la suppression de vos AWS ressources.

AWS Serverless Application Model (AWS SAM)

AWS SAM est un framework open source construit sur. CloudFormation Il fournit une syntaxe simplifiée pour définir les applications sans serveur. Utilisez des modèles AWS SAM pour configurer rapidement des fonctions Lambda, des API, des bases de données et des sources d'événements avec seulement quelques lignes de code YAML.

Cloud Development Kit AWS (AWS CDK)

Le CDK est une approche d'IaC axée sur le code. Vous pouvez définir votre Lambda-based architecture à l'aide de Python TypeScript JavaScript, Java, C#/.NET ou Go. Choisissez votre langage préféré et utilisez des éléments de programmation tels que les paramètres, les conditions, les boucles, la composition et l'héritage pour définir le résultat souhaité pour votre infrastructure. Le CDK génère ensuite les CloudFormation modèles sous-jacents pour le déploiement. Pour obtenir un exemple d'utilisation de Lambda avec CDK, consultez Déploiement de fonctions événementielles avec AWS CDK.



AWS fournit également un service appelé AWS Infrastructure Composer à développer des modèles IaC à l'aide d'une interface graphique simple. Avec Infrastructure Composer, vous concevez une architecture d'application en faisant glisser, en regroupant et Services AWS en connectant dans un canevas visuel. Infrastructure Composer crée ensuite un AWS SAM modèle ou un CloudFormation modèle à partir de votre conception que vous pouvez utiliser pour déployer votre application.

Dans la section the section called "Utilisation d' AWS SAM un compositeur d'infrastructure" ci-dessous, Infrastructure Composer vous permet de développer un modèle pour une application sans serveur basée sur une fonction Lambda existante.

Utilisation des fonctions événementielles dans AWS SAM et Compositeur d'infrastructure

Dans ce didacticiel, vous pouvez commencer à utiliser IaC avec Lambda en créant un AWS SAM modèle à partir d'une fonction Lambda existante, puis en développant une application sans serveur dans Infrastructure Composer en ajoutant d'autres ressources. AWS

Au cours de ce didacticiel, vous apprendrez certains concepts fondamentaux, tels que la manière dont les AWS ressources sont spécifiées dans AWS SAM. Vous apprendrez également à utiliser Infrastructure Composer pour créer une application sans serveur que vous pouvez déployer à l'aide de AWS SAM ou CloudFormation.

Pour terminer ce didacticiel, vous allez suivre les étapes suivantes :

- Créer un exemple de fonction Lambda
- Utilisez la console Lambda pour afficher le AWS SAM modèle de la fonction
- Exportez la configuration de votre fonction vers une application sans serveur simple AWS Infrastructure Composer et concevez une application sans serveur basée sur la configuration de votre fonction
- Enregistrez un AWS SAM modèle mis à jour que vous pouvez utiliser comme base pour déployer votre application sans serveur

Conditions préalables

Dans ce didacticiel, vous utiliserez la fonction de synchronisation locale d'Infrastructure Composer pour enregistrer vos modèles et vos fichiers de code sur votre machine de génération locale. Pour utiliser cette fonctionnalité, vous devez disposer d’un navigateur compatible avec l’API d’accès au système de fichiers, qui permet aux applications Web de lire, d’écrire et d’enregistrer des fichiers dans votre système de fichiers local. Nous vous recommandons d’utiliser Google Chrome ou Microsoft Edge. Pour plus d’informations sur l’API d’accès au système de fichiers, voir Qu’est-ce que l’API d’accès au système de fichiers ?

Création d'une fonction événementielle

Dans cette première étape, vous allez créer une fonction Lambda que vous pouvez utiliser pour terminer le reste du didacticiel. Pour simplifier les choses, vous utilisez la console Lambda pour créer une fonction de base « Hello world » à l’aide du moteur d’exécution Python 3.11.

Pour créer une fonction d'événement « Hello world » à l'aide de la console

1. Ouvrez la console Lambda.
2. Choisissez Create Event Function.
3. Ne désélectionnez pas l'option Créer à partir de zéro puis, sous Informations de base, saisissez **`LambdaIaCDemo`** pour le nom de la fonction.
4. Pour l'environnement d'exécution, sélectionnez Python 3.11.
5. Choisissez Create Event Function.

Consultez le AWS SAM modèle pour votre fonction

Avant d'exporter la configuration de votre fonction vers Infrastructure Composer, utilisez la console Lambda pour afficher la configuration actuelle de votre fonction sous forme de modèle AWS SAM . En suivant les étapes décrites dans cette section, vous découvrirez l'anatomie d'un AWS SAM modèle et comment définir des ressources telles que les fonctions Lambda pour commencer à spécifier une application sans serveur.

Pour consulter le AWS SAM modèle pour votre fonction

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez la fonction que vous venez de créer (`LambdaIaCDemo`).
3. Dans le volet de Présentation de la fonction, choisissez Modèle.

   À la place du schéma représentant la configuration de votre fonction, vous verrez un AWS SAM modèle pour votre fonction. Le modèle doit ressembler à ce qui suit.

```
# This AWS SAM template has been generated from your function's
# configuration. If your function has one or more triggers, note
# that the AWS resources associated with these triggers aren't fully
# specified in this template and include placeholder values.Open this template
# in AWS Application Composer or your favorite IDE and modify
# it to specify a serverless application with other AWS resources.
AWSTemplateFormatVersion: '2010-09-09'
Transform: AWS::Serverless-2016-10-31
Description: An AWS Serverless Specification template describing your function.
Resources:
  LambdaIaCDemo:
    Type: AWS::Serverless::Function
    Properties:
```

```
      CodeUri: .
      Description: ''
      MemorySize: 128
      Timeout: 3
      Handler: lambda_function.lambda_handler
      Runtime: python3.11
      Architectures:
        - x86_64
      EventInvokeConfig:
        MaximumEventAgeInSeconds: 21600
        MaximumRetryAttempts: 2
      EphemeralStorage:
        Size: 512
      RuntimeManagementConfig:
        UpdateRuntimeOn: Auto
      SnapStart:
        ApplyOn: None
      PackageType: Zip
      Policies:
        Statement:
          - Effect: Allow
            Action:
              - logs:CreateLogGroup
            Resource: arn:aws:logs:us-east-1:123456789012:*
          - Effect: Allow
            Action:
              - logs:CreateLogStream
              - logs:PutLogEvents
            Resource:
              - >-
                arn:aws:logs:us-east-1:123456789012:log-group:/aws/lambda/
LambdaIaCDemo:*
```

Prenons un moment pour examiner le modèle YAML de votre fonction et comprendre certains concepts clés.

Le modèle commence par la déclaration `Transform: AWS::Serverless-2016-10-31`. Cette déclaration est obligatoire car, dans les coulisses, les AWS SAM modèles sont déployés via CloudFormation. L'utilisation de l'instruction `Transform` identifie le modèle en tant que fichier modèle AWS SAM .

Après la déclaration `Transform` vient la section `Resources`. C'est ici que sont définies les AWS ressources que vous souhaitez déployer avec votre AWS SAM modèle. AWS SAM les modèles peuvent contenir une combinaison de AWS SAM ressources et de CloudFormation ressources. Cela est dû au fait que pendant le déploiement, les AWS SAM CloudFormation modèles se transforment en modèles, de sorte que toute CloudFormation syntaxe valide peut être ajoutée à un AWS SAM modèle.

Pour le moment, une seule ressource est définie dans la section `Resources` du modèle, votre fonction Lambda `LambdaIaCDemo`. Pour ajouter une fonction Lambda à un AWS SAM modèle, vous devez utiliser le type de `AWS::Serverless::Function` ressource. La ressource `Properties` d'une fonction Lambda définit l'exécution de la fonction, le gestionnaire de fonctions et les autres options de configuration. Le chemin d'accès au code source de votre fonction qui AWS SAM doit être utilisé pour déployer la fonction est également défini ici. Pour en savoir plus sur les ressources relatives aux fonctions Lambda dans AWS SAM, voir AWS::Serverless::Function dans le manuel du AWS SAM développeur.

Outre les propriétés et les configurations des fonctions, le modèle spécifie également une politique Gestion des identités et des accès AWS (IAM) pour votre fonction. Cette politique autorise votre fonction à écrire des journaux sur Amazon CloudWatch Logs. Lorsque vous créez une fonction dans la console Lambda, Lambda associe automatiquement cette politique à votre fonction. Pour en savoir plus sur la spécification d'une politique IAM pour une fonction dans un AWS SAM modèle, consultez la `policies` propriété sur la page AWS::Serverless::Function du manuel du AWS SAM développeur.

Pour en savoir plus sur la structure des AWS SAM modèles, consultez la section Anatomie des AWS SAM modèles.

Utilisation AWS Infrastructure Composer pour concevoir une application sans serveur

Pour commencer à créer une application sans serveur simple en utilisant le AWS SAM modèle de votre fonction comme point de départ, vous exportez la configuration de votre fonction vers Infrastructure Composer et activez le mode de synchronisation local d'Infrastructure Composer. La synchronisation locale enregistre automatiquement le code de votre fonction et votre AWS SAM modèle sur votre machine de génération locale et synchronise votre modèle enregistré lorsque vous ajoutez d'autres AWS ressources dans Infrastructure Composer.

Pour exporter votre fonction vers Infrastructure Composer

1. Dans le volet Vue d’ensemble des fonctions, choisissez Exporter vers Application Composer.

Pour exporter la configuration et le code de votre fonction vers Infrastructure Composer, Lambda crée un compartiment Amazon S3 dans votre compte pour stocker temporairement ces données.

2. Dans la boîte de dialogue, choisissez Confirmer et créer un projet pour accepter le nom par défaut de ce compartiment et exporter la configuration et le code de votre fonction vers Infrastructure Composer.
3. (Facultatif) Pour choisir un autre nom pour le compartiment Amazon S3 créé par Lambda, entrez un nouveau nom et choisissez Confirmer et créer un projet. Les noms de compartiment Amazon S3 doivent être uniques et respecter les règles de dénomination de compartiment.

   Sélectionnez Confirmer et créer un projet pour ouvrir la console Infrastructure Composer. Sur le canevas, vous verrez votre fonction Lambda.
4. Dans le menu déroulant, choisissez Activer la synchronisation locale.
5. Dans la boîte de dialogue qui apparaît, choisissez Sélectionner un dossier et un dossier sur votre machine de construction locale.
6. Choisissez Activer pour activer la synchronisation locale.

Pour exporter votre fonction vers Infrastructure Composer, vous avez besoin d'une autorisation pour utiliser certaines actions d'API. Si vous ne parvenez pas à exporter votre fonction, vérifiez the section called "Autorisations requises" et assurez-vous que vous disposez des autorisations nécessaires.

> **Note**
>
> La tarification standard d'Amazon S3 s'applique au compartiment créé par Lambda lorsque vous exportez une fonction vers Infrastructure Composer. Les objets que Lambda place dans le compartiment sont automatiquement supprimés au bout de 10 jours, mais Lambda ne supprime pas le compartiment lui-même.
> Pour éviter que des frais supplémentaires ne soient ajoutés à votre Compte AWS compte, suivez les instructions de la section Supprimer un bucket après avoir exporté votre fonction vers Infrastructure Composer. Pour en savoir plus sur le compartiment Amazon S3 créé par Lambda, consultez the section called "Compositeur d'infrastructure".

Pour concevoir votre application sans serveur dans Infrastructure Composer

Après avoir activé la synchronisation locale, les modifications que vous apportez dans Infrastructure Composer sont reflétées dans le AWS SAM modèle enregistré sur votre machine de génération

locale. Vous pouvez désormais glisser-déposer des AWS ressources supplémentaires sur le canevas Infrastructure Composer pour créer votre application. Dans cet exemple, vous ajoutez une file d'attente simple Amazon SQS comme déclencheur pour votre fonction Lambda et une table DynamoDB pour la fonction dans laquelle écrire des données.

1. Ajoutez un déclencheur Amazon SQS à votre fonction Lambda en procédant comme suit :

   a. Dans le champ de recherche de la palette Ressources, entrez **`SQS`**.

   b. Faites glisser la ressource SQS Queue sur votre canevas et positionnez-la à gauche de votre fonction Lambda.

   c. Choisissez Détails, puis, pour Logical ID, entrez **`LambdaIaCQueue`**.

   d. Cliquez sur Enregistrer.

   e. Connectez vos ressources Amazon SQS et Lambda en cliquant sur le port Abonnement sur la carte de file d'attente SQS et en le faisant glisser vers le port gauche de la carte de fonction Lambda. L'apparition d'une ligne entre les deux ressources indique que la connexion a abouti. Infrastructure Composer affiche également un message au bas du canevas indiquant que les deux ressources sont correctement connectées.

2. Ajoutez une table Amazon DynamoDB dans laquelle votre fonction Lambda pourra y écrire des données en procédant comme suit :

   a. Dans le champ de recherche de la palette Ressources, entrez **`DynamoDB`**.

   b. Faites glisser la ressource Table DynamoDB sur votre canevas et positionnez-la à droite de votre fonction Lambda.

   c. Choisissez Détails, puis, pour Logical ID, entrez **`LambdaIaCTable`**.

   d. Cliquez sur Enregistrer.

   e. Connectez la table DynamoDB à votre fonction Lambda en cliquant sur le port droit de la carte de fonction Lambda et en la faisant glisser vers le port gauche de la carte DynamoDB.

Maintenant que vous avez ajouté ces ressources supplémentaires, examinons le AWS SAM modèle mis à jour créé par Infrastructure Composer.

Pour consulter vos mises à jour AWS SAM modèle

- Sur le canevas Infrastructure Composer, choisissez Modèle pour passer de la vue canevas à la vue modèle.

Votre AWS SAM modèle doit désormais contenir les ressources et propriétés supplémentaires suivantes :

- File d'attente Amazon SQS avec l'identifiant `LambdaIaCQueue`

```
LambdaIaCQueue:
    Type: AWS::SQS::Queue
    Properties:
      MessageRetentionPeriod: 345600
```

  Lorsque vous ajoutez une file d'attente Amazon SQS à l'aide d'Infrastructure Composer, Infrastructure Composer définit la propriété `MessageRetentionPeriod`. Vous pouvez également définir la propriété `FifoQueue` en sélectionnant Détails sur la carte SQS Queue et en cochant ou décochant la file d'attente Fifo.

  Pour définir d'autres propriétés pour votre file d'attente, vous pouvez modifier manuellement le modèle et les y ajouter. Pour en savoir plus sur la ressource `AWS::SQS::Queue` et ses propriétés disponibles, consultez AWS::SQS::Queue dans le Guide de l'utilisateur CloudFormation .

- Propriété `Events` de votre définition de fonction Lambda qui spécifie la file d'attente Amazon SQS comme déclencheur de la fonction

```
Events:
  LambdaIaCQueue:
    Type: SQS
    Properties:
      Queue: !GetAtt LambdaIaCQueue.Arn
      BatchSize: 1
```

  La propriété `Events` est constituée d'un type d'événement et d'un ensemble de propriétés qui dépendent du type. Pour en savoir plus sur les différentes options Services AWS que vous pouvez configurer pour déclencher une fonction Lambda et sur les propriétés que vous pouvez définir, consultez le EventSourceguide du AWS SAM développeur.

- Table DynamoDB avec l'identifiant `LambdaIaCTable`

```
LambdaIaCTable:
    Type: AWS::DynamoDB::Table
    Properties:
      AttributeDefinitions:
        - AttributeName: id
```

```
          AttributeType: S
      BillingMode: PAY_PER_REQUEST
      KeySchema:
        - AttributeName: id
          KeyType: HASH
      StreamSpecification:
        StreamViewType: NEW_AND_OLD_IMAGES
```

Lorsque vous ajoutez une table DynamoDB à l'aide d'Infrastructure Composer, vous pouvez définir les clés de votre table en choisissant Détails sur la fiche de table DynamoDB et en modifiant les valeurs clés. Infrastructure Composer définit également des valeurs par défaut pour un certain nombre d'autres propriétés, notamment `BillingMode` et `StreamViewType`.

Pour en savoir plus sur ces propriétés et les autres propriétés que vous pouvez ajouter à votre AWS SAM modèle, consultez AWS: :DynamoDB : :Table dans le guide de l'utilisateur.CloudFormation

- Une nouvelle politique IAM qui autorise votre fonction à effectuer des opérations CRUD sur la table DynamoDB que vous avez ajoutée.

```
Policies:
...
  - DynamoDBCrudPolicy:
    TableName: !Ref LambdaIaCTable
```

Le AWS SAM modèle final complet doit ressembler à ce qui suit.

```
AWSTemplateFormatVersion: '2010-09-09'
Transform: AWS::Serverless-2016-10-31
Description: An AWS Serverless Specification template describing your function.
Resources:
  LambdaIaCDemo:
    Type: AWS::Serverless::Function
    Properties:
      CodeUri: .
      Description: ''
      MemorySize: 128
      Timeout: 3
      Handler: lambda_function.lambda_handler
      Runtime: python3.11
      Architectures:
```

```
        - x86_64
      EventInvokeConfig:
        MaximumEventAgeInSeconds: 21600
        MaximumRetryAttempts: 2
      EphemeralStorage:
        Size: 512
      RuntimeManagementConfig:
        UpdateRuntimeOn: Auto
      SnapStart:
        ApplyOn: None
      PackageType: Zip
      Policies:
        - Statement:
            - Effect: Allow
              Action:
                - logs:CreateLogGroup
              Resource: arn:aws:logs:us-east-1:594035263019:*
            - Effect: Allow
              Action:
                - logs:CreateLogStream
                - logs:PutLogEvents
              Resource:
                - arn:aws:logs:us-east-1:594035263019:log-group:/aws/lambda/
LambdaIaCDemo:*
        - DynamoDBCrudPolicy:
            TableName: !Ref LambdaIaCTable
      Events:
        LambdaIaCQueue:
          Type: SQS
          Properties:
            Queue: !GetAtt LambdaIaCQueue.Arn
            BatchSize: 1
      Environment:
        Variables:
          LAMBDAIACTABLE_TABLE_NAME: !Ref LambdaIaCTable
          LAMBDAIACTABLE_TABLE_ARN: !GetAtt LambdaIaCTable.Arn
  LambdaIaCQueue:
    Type: AWS::SQS::Queue
    Properties:
      MessageRetentionPeriod: 345600
  LambdaIaCTable:
    Type: AWS::DynamoDB::Table
    Properties:
      AttributeDefinitions:
```

```
        - AttributeName: id
          AttributeType: S
      BillingMode: PAY_PER_REQUEST
      KeySchema:
        - AttributeName: id
          KeyType: HASH
      StreamSpecification:
        StreamViewType: NEW_AND_OLD_IMAGES
```

Déployez votre application sans serveur à l'aide de AWS SAM (facultatif)

Si vous souhaitez déployer une application sans serveur AWS SAM à l'aide du modèle que vous venez de créer dans Infrastructure Composer, vous devez d'abord installer le AWS SAM CLI. Pour ce faire, suivez les instructions de la section Installation de la AWS SAM CLI.

Avant de déployer votre application, vous devez également mettre à jour le code de fonction enregistré par Infrastructure Composer avec votre modèle. Pour le moment, le fichier `lambda_function.py` enregistré par Infrastructure Composer ne contient que le code de base « Hello world » fourni par Lambda lors de la création de la fonction.

Pour mettre à jour votre code de fonction, copiez le code suivant et collez-le dans le fichier `lambda_function.py` qu'Infrastructure Composer a enregistré sur votre machine de compilation locale. Vous avez spécifié le répertoire dans lequel Infrastructure Composer doit enregistrer ce fichier lorsque vous avez activé le mode de synchronisation locale.

Ce code accepte une paire clé-valeur dans un message provenant de la file d'attente Amazon SQS que vous avez créée dans Infrastructure Composer. Si la clé et la valeur sont des chaînes, le code les utilise ensuite pour écrire un élément dans la table DynamoDB définie dans votre modèle.

Mise à jour du code de la fonction Python

```
import boto3
import os
import json

# define the DynamoDB table that Lambda will connect to
tablename = os.environ['LAMBDAIACTABLE_TABLE_NAME']

# create the DynamoDB resource
dynamo = boto3.client('dynamodb')
```

```
def lambda_handler(event, context):
    # get the message out of the SQS event
    message = event['Records'][0]['body']
    data = json.loads(message)
    # write event data to DDB table
    if check_message_format(data):
        key = next(iter(data))
        value = data[key]
        dynamo.put_item(
            TableName=tablename,
            Item={
                'id': {'S': key},
                'Value': {'S': value}
            }
        )
    else:
        raise ValueError("Input data not in the correct format")

# check that the event object contains a single key value
# pair that can be written to the database
def check_message_format(message):
    if len(message) != 1:
        return False

    key, value = next(iter(message.items()))

    if not (isinstance(key, str) and isinstance(value, str)):
        return False

    else:
        return True
```

Pour déployer votre application sans serveur

Pour déployer votre application à l'aide du AWS SAM CLI, procédez comme suit. Pour que votre fonction soit correctement construite et déployée, la version 3.11 de Python doit être installée sur votre machine de compilation et sur votre PATH.

1. Exécutez la commande suivante depuis le répertoire dans lequel Infrastructure Composer a enregistré vos fichiers `template.yaml` et `lambda_function.py`.

   ```
   sam build
   ```

Cette commande rassemble les artefacts de compilation pour votre application et les place dans le format et l'emplacement appropriés pour les déployer.

2. Pour déployer votre application et créer les ressources Lambda, Amazon SQS et DynamoDB spécifiées dans AWS SAM votre modèle, exécutez la commande suivante.

```
sam deploy --guided
```

L'utilisation du `--guided` drapeau signifie que des instructions vous AWS SAM seront affichées pour vous guider tout au long du processus de déploiement. Pour ce déploiement, acceptez les options par défaut en appuyant sur Entrée.

Au cours du processus de déploiement, AWS SAM crée les ressources suivantes dans votre Compte AWS :

- Une CloudFormation pile nommée `sam-app`
- Une fonction Lambda avec le format de nom `sam-app-LambdaIaCDemo-99VXPpYQVv1M`
- Une file d'attente Amazon SQS au format de nom `sam-app-LambdaIaCQueue-xL87VeKsGiIo`
- Une table DynamoDB au format de nom `sam-app-LambdaIaCTable-CN0S66C0VLNV`

AWS SAM crée également les rôles et politiques IAM nécessaires pour que votre fonction Lambda puisse lire les messages de la file d'attente Amazon SQS et effectuer des opérations CRUD sur la table DynamoDB.

Testing de votre application déployée (facultatif)

Pour vérifier que votre application sans serveur s'est déployée correctement, envoyez un message à votre file d'attente Amazon SQS contenant une paire clé-valeur et vérifiez que Lambda écrit un élément dans votre table DynamoDB en utilisant ces valeurs.

Tester votre application sans serveur

1. Ouvrez la page Files d'attente de la console Amazon SQS et sélectionnez la file d'attente créée par AWS SAM depuis votre modèle. Le nom est au format `sam-app-LambdaIaCQueue-xL87VeKsGiIo`.
2. Choisissez Envoyer et recevoir des messages, puis collez le code JSON suivant dans le champ Corps du message, dans la section Envoyer un message.

```
{
    "myKey": "myValue"
}
```

3. Choisissez Send Message (Envoyer un message).

   L'envoi de votre message à la file d'attente amène Lambda à invoquer votre fonction par le biais du mappage de la source d'événement défini dans votre modèle AWS SAM . Pour confirmer que Lambda a invoqué votre fonction comme prévu, indiquez qu'un élément a été ajouté à votre table DynamoDB.
4. Ouvrez la page Tables de la console DynamoDB et choisissez votre table. Le nom est au format `sam-app-LambdaIaCTable-CN0S66C0VLNV`.
5. Sélectionnez Explorer les éléments de table. Dans le volet Items returned (Éléments retournés), vous devriez voir un élément avec l'id `myKey` et la Valeur `myValue`.

Déploiement de fonctions événementielles avec AWS CDK

Cloud Development Kit AWS (AWS CDK) Il s'agit d'un framework d'infrastructure en tant que code (IaC) que vous pouvez utiliser pour définir une infrastructure AWS cloud en utilisant le langage de programmation de votre choix. Pour définir votre propre infrastructure de cloud, écrivez d'abord une application (dans l'un des langages pris en charge par le CDK) contenant une ou plusieurs piles. Ensuite, vous le synthétisez dans un CloudFormation modèle et déployez vos ressources sur votre Compte AWS. Suivez les étapes décrites dans cette rubrique pour déployer une fonction d'événement Lambda qui renvoie un événement depuis un point de terminaison Amazon API Gateway.

La bibliothèque AWS Construct, incluse dans le CDK, fournit des modules que vous pouvez utiliser pour modéliser les ressources Services AWS fournies. Pour les services populaires, la bibliothèque fournit des constructions organisées avec des valeurs par défaut intelligentes et les bonnes pratiques. Vous pouvez utiliser le module aws_lambda pour définir votre fonction et les ressources de support en quelques lignes de code.

Conditions préalables

Avant de commencer ce didacticiel, installez le AWS CDK en exécutant la commande suivante.

```
npm install -g aws-cdk
```

Étape 1 : Configurez votre AWS CDK project

Créez un répertoire pour votre nouvelle AWS CDK application et initialisez le projet.

JavaScript

```
mkdir hello-lambda
cd hello-lambda
cdk init --language javascript
```

TypeScript

```
mkdir hello-lambda
cd hello-lambda
cdk init --language typescript
```

Python

```
mkdir hello-lambda
cd hello-lambda
cdk init --language python
```

Une fois le projet démarré, activez l'environnement virtuel du projet et installez les dépendances de base d' AWS CDK.

```
source .venv/bin/activate
python -m pip install -r requirements.txt
```

Java

```
mkdir hello-lambda
cd hello-lambda
cdk init --language java
```

Importez ce projet Maven dans votre environnement de développement intégré (IDE) Java. Par exemple, dans Eclipse, utilisez Fichier, Importer, Maven, Projets Maven existants.

C#

```
mkdir hello-lambda
```

```
cd hello-lambda
cdk init --language csharp
```

> **Note**
>
> Le modèle AWS CDK d'application utilise le nom du répertoire du projet pour générer des noms pour les classes et les fichiers sources. Dans cet exemple, le répertoire est nommé `hello-lambda`. Si vous utilisez un nom répertoire différent, votre application ne correspondra pas à ces instructions.

AWS CDK v2 inclut des constructions stables pour tous Services AWS dans un seul package appelé`aws-cdk-lib`. Ce package est installé en tant que dépendance lorsque vous initialisez le projet. Lorsque vous travaillez avec certains langages de programmation, le package est installé lorsque vous créez le projet pour la première fois.

Étape 2 : définir le AWS CDK pile

Une pile CDK est un ensemble d'une ou plusieurs constructions qui définissent AWS les ressources. Chaque pile CDK représente une CloudFormation pile dans votre application CDK.

Pour définir votre pile CDK, suivez les instructions de votre langage de programmation préféré. Cette pile définit les éléments suivants :

- Le nom logique de la fonction : `MyFunction`
- L'emplacement du code de fonction, spécifié dans la propriété `code`. Pour plus d'informations, consultez Handler code dans la Référence de l'API Cloud Development Kit AWS (AWS CDK) .
- Le nom logique de l'API REST : `HelloApi`
- Le nom logique du point de terminaison d'API Gateway : `ApiGwEndpoint`

Notez que toutes les piles CDK de ce didacticiel utilisent le Node.js runtime de la fonction Lambda. Vous pouvez utiliser différents langages de programmation pour la pile CDK et la fonction Lambda afin d'exploiter les points forts de chaque langage. Par exemple, vous pouvez utiliser la pile CDK TypeScript pour tirer parti des avantages du typage statique pour votre code d'infrastructure. Vous pouvez utiliser la fonction Lambda JavaScript pour tirer parti de la flexibilité et du développement rapide d'un langage typé dynamiquement.

JavaScript

Ouvrez le fichier `lib/hello-lambda-stack.js` et remplacez le contenu par ce qui suit.

```
const { Stack } = require('aws-cdk-lib');
const lambda = require('aws-cdk-lib/aws-lambda');
const apigw = require('aws-cdk-lib/aws-apigateway');

class HelloLambdaStack extends Stack {
  /**
   *
   * @param {Construct} scope
   * @param {string} id
   * @param {StackProps=} props
   */
  constructor(scope, id, props) {
    super(scope, id, props);
    const fn = new lambda.Function(this, 'MyFunction', {
      code: lambda.Code.fromAsset('lib/lambda-handler'),
      runtime: lambda.Runtime.NODEJS_LATEST,
      handler: 'index.handler'
    });

    const endpoint = new apigw.LambdaRestApi(this, 'MyEndpoint', {
      handler: fn,
      restApiName: "HelloApi"
    });

  }
}

module.exports = { HelloLambdaStack }
```

TypeScript

Ouvrez le fichier `lib/hello-lambda-stack.ts` et remplacez le contenu par ce qui suit.

```
import * as cdk from 'aws-cdk-lib';
import { Construct } from 'constructs';
import * as apigw from "aws-cdk-lib/aws-apigateway";
import * as lambda from "aws-cdk-lib/aws-lambda";
import * as path from 'node:path';
```

```
export class HelloLambdaStack extends cdk.Stack {
  constructor(scope: Construct, id: string, props?: cdk.StackProps){
    super(scope, id, props)
    const fn = new lambda.Function(this, 'MyFunction', {
      runtime: lambda.Runtime.NODEJS_LATEST,
      handler: 'index.handler',
      code: lambda.Code.fromAsset(path.join(__dirname, 'lambda-handler')),
    });

    const endpoint = new apigw.LambdaRestApi(this, `ApiGwEndpoint`, {
      handler: fn,
      restApiName: `HelloApi`,
    });

  }
}
```

Python

Ouvrez le fichier `/hello-lambda/hello_lambda/hello_lambda_stack.py` et remplacez le contenu par ce qui suit.

```
from aws_cdk import (
    Stack,
    aws_apigateway as apigw,
    aws_lambda as _lambda
)
from constructs import Construct

class HelloLambdaStack(Stack):

    def __init__(self, scope: Construct, construct_id: str, **kwargs) -> None:
        super().__init__(scope, construct_id, **kwargs)

        fn = _lambda.Function(
            self,
            "MyFunction",
            runtime=_lambda.Runtime.NODEJS_LATEST,
            handler="index.handler",
            code=_lambda.Code.from_asset("lib/lambda-handler")
        )

        endpoint = apigw.LambdaRestApi(
```

```
            self,
            "ApiGwEndpoint",
            handler=fn,
            rest_api_name="HelloApi"
        )
```

Java

Ouvrez le fichier `/hello-lambda/src/main/java/com/myorg/HelloLambdaStack.java` et remplacez le contenu par ce qui suit.

```
package com.myorg;

import software.constructs.Construct;
import software.amazon.awscdk.Stack;
import software.amazon.awscdk.StackProps;
import software.amazon.awscdk.services.apigateway.LambdaRestApi;
import software.amazon.awscdk.services.lambda.Function;

public class HelloLambdaStack extends Stack {
    public HelloLambdaStack(final Construct scope, final String id) {
        this(scope, id, null);
    }

    public HelloLambdaStack(final Construct scope, final String id, final StackProps
 props) {
        super(scope, id, props);

        Function hello = Function.Builder.create(this, "MyFunction")

 .runtime(software.amazon.awscdk.services.lambda.Runtime.NODEJS_LATEST)

 .code(software.amazon.awscdk.services.lambda.Code.fromAsset("lib/lambda-handler"))
                            .handler("index.handler")
                            .build();

        LambdaRestApi api = LambdaRestApi.Builder.create(this, "ApiGwEndpoint")
                                .restApiName("HelloApi")
                                .handler(hello)
                                .build();

    }
}
```

C#

Ouvrez le fichier `src/HelloLambda/HelloLambdaStack.cs` et remplacez le contenu par ce qui suit.

```
using Amazon.CDK;
using Amazon.CDK.AWS.APIGateway;
using Amazon.CDK.AWS.Lambda;
using Constructs;

namespace HelloLambda
{
    public class HelloLambdaStack : Stack
    {
        internal HelloLambdaStack(Construct scope, string id, IStackProps props =
 null) : base(scope, id, props)
        {
            var fn = new Function(this, "MyFunction", new FunctionProps
            {
                Runtime = Runtime.NODEJS_LATEST,
                Code = Code.FromAsset("lib/lambda-handler"),
                Handler = "index.handler"
            });

            var api = new LambdaRestApi(this, "ApiGwEndpoint", new
 LambdaRestApiProps
            {
                Handler = fn
            });
        }
    }
}
```

Étape 3 : Création du code de la fonction d'événement

1. À partir de la racine de votre projet (`hello-lambda`), créez le répertoire `/lib/lambda-handler` pour le code de la fonction Lambda. Ce répertoire est spécifié dans la `code` propriété de votre AWS CDK pile.
2. Dans le répertoire `/lib/lambda-handler`, créez un nouveau fichier appelé `index.js`. Collez le code suivant dans le fichier. La fonction extrait des propriétés spécifiques de la requête d'API et les renvoie sous forme de réponse JSON.

```
exports.handler = async (event) => {
  // Extract specific properties from the event object
  const { resource, path, httpMethod, headers, queryStringParameters, body } =
 event;
  const response = {
    resource,
    path,
    httpMethod,
    headers,
    queryStringParameters,
    body,
  };
  return {
    body: JSON.stringify(response, null, 2),
    statusCode: 200,
  };
};
```

Étape 4 : Déployez le AWS CDK pile

1. À la racine de votre projet, effectuez la commande cdk synth :

   ```
   cdk synth
   ```

   Cette commande synthétise un AWS CloudFormation modèle à partir de votre pile de CDK. Le modèle est un fichier YAML d'environ 400 lignes, semblable à ce qui suit.

   > **Note**
   >
   > Si vous obtenez l'erreur suivante, assurez-vous que vous êtes à la racine du répertoire de votre projet.
   >
   > ```
   > --app is required either in command-line, in cdk.json or in ~/.cdk.json
   > ```

   Example CloudFormation modèle

   ```
   Resources:
   ```

```
  MyFunctionServiceRole3C357FF2:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Statement:
          - Action: sts:AssumeRole
            Effect: Allow
            Principal:
              Service: lambda.amazonaws.com
        Version: "2012-10-17"
      ManagedPolicyArns:
        - Fn::Join:
            - ""
            - - "arn:"
              - Ref: AWS::Partition
              - :iam::aws:policy/service-role/AWSLambdaBasicExecutionRole
    Metadata:
      aws:cdk:path: HelloLambdaStack/MyFunction/ServiceRole/Resource
  MyFunction1BAA52E7:
    Type: AWS::Lambda::Function
    Properties:
      Code:
        S3Bucket:
          Fn::Sub: cdk-hnb659fds-assets-${AWS::AccountId}-${AWS::Region}
        S3Key:
ab1111111cd32708dc4b83e81a21c296d607ff2cdef00f1d7f48338782f92l3901.zip
      Handler: index.handler
      Role:
        Fn::GetAtt:
          - MyFunctionServiceRole3C357FF2
          - Arn
      Runtime: nodejs24.x
      ...
```

2. Exécutez la commande cdk deploy :

```
cdk deploy
```

Patientez que vos ressources soient créées. Le résultat final inclut l'URL de votre point de terminaison d'API Gateway. Exemple :

```
Outputs:
```

```
HelloLambdaStack.ApiGwEndpoint77F417B1 = https://abcd1234.execute-api.us-
east-1.amazonaws.com/prod/
```

Étape 5 : tester de la fonction

Pour invoquer la fonction Lambda, copiez le point de terminaison d'API Gateway et collez-le dans un navigateur Web ou exécutez une commande `curl` :

```
curl -s https://abcd1234.execute-api.us-east-1.amazonaws.com/prod/
```

La réponse est une représentation JSON des propriétés sélectionnées à partir de l'objet d'événement d'origine, qui contient des informations sur la requête envoyée au point de terminaison d'API Gateway. Exemple :

```
{
  "resource": "/",
  "path": "/",
  "httpMethod": "GET",
  "headers": {
    "Accept": "text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7",
    "Accept-Encoding": "gzip, deflate, br, zstd",
    "Accept-Language": "en-US,en;q=0.9",
    "CloudFront-Forwarded-Proto": "https",
    "CloudFront-Is-Desktop-Viewer": "true",
    "CloudFront-Is-Mobile-Viewer": "false",
    "CloudFront-Is-SmartTV-Viewer": "false",
    "CloudFront-Is-Tablet-Viewer": "false",
    "CloudFront-Viewer-ASN": "16509",
    "CloudFront-Viewer-Country": "US",
    "Host": "abcd1234.execute-api.us-east-1.amazonaws.com",
     ...
```

Étape 6 : Nettoyer vos ressources

Le point de terminaison d'API Gateway est accessible au public. Pour éviter des frais inattendus, exécutez la commande cdk destroy pour supprimer la pile et toutes les ressources associées.

```
cdk destroy
```

Étapes suivantes

Pour plus d'informations sur l'écriture d' AWS CDK applications dans la langue de votre choix, consultez les rubriques suivantes :

TypeScript

- Travailler avec le AWS CDK in TypeScript

JavaScript

- Travailler avec le AWS CDK in JavaScript

Python

- Travailler avec le AWS CDK en Python

Java

- Travailler avec le AWS CDK en Java

C#

- Travailler avec le AWS CDK en C#

Go

- Travailler avec le AWS CDK in Go

Outils électriques pour AWS Lambda

Powertools for AWS Lambda (également appelé Powertools AWS pour) fournit des fonctions utilitaires, des décorateurs et des intergiciels qui gèrent les tâches Lambda courantes telles que la journalisation structurée, le traçage, la collecte de métriques et la validation des entrées. Utilisez Powertools for AWS Lambda pour mettre en œuvre les meilleures pratiques sans serveur et accélérer le développement de plusieurs fonctions d'événement Lambda. Vous simplifierez ainsi les tâches de développement courantes dans vos fonctions Lambda.

Principaux avantages de Powertools pour AWS

Bien que le développement Lambda soit possible sans Powertools for AWS, son utilisation présente plusieurs avantages :

- Built-in observabilité : journalisation structurée, suivi et mesures personnalisées
- Gestion des secrets : récupération des paramètres, gestion des secrets et idempotence
- Amélioration progressive : choisissez les utilitaires qui répondent le mieux à vos besoins
- Développement accéléré : analyse des événements, validation et traitement par lots
- Bonnes pratiques : mise en œuvre de AWS Well-Architected modèles sans serveur

Intégration de Powertools à AWS

Powertools for vous AWS aide à créer des applications sans serveur prêtes pour la production avec moins de code personnalisé. Disponible en Python TypeScript/Node.js, .NET et Java, Powertools for AWS peut être inclus via Lambda Layers ou à l'aide du gestionnaire de packages linguistiques. Chaque implémentation de langage fournit des fonctionnalités de base, comme la journalisation structurée, le suivi, la collecte de métriques et la gestion des événements, tout en conservant les expressions idiomatiques propres à chaque langage de programmation. Ces implémentations sont complétées par des composants spécialisés pour l'intégration des AWS services, la prise en charge de la récupération des paramètres, le traitement par lots et la gestion des API, ainsi que par les meilleures pratiques telles que la propagation des identifiants de corrélation, la gestion des erreurs et les modèles d'idempuissance. Ensemble, ces fonctionnalités permettent aux développeurs de créer des applications sans serveur robustes et faciles à maintenir tout en réduisant la charge liée au code personnalisé.

- Powertools pour AWS Lambda (Python)
- Outils électriques pour AWS TypeScript Lambda ()
- Outils électriques pour AWS Lambda (Java)
- Outils électriques pour AWS Lambda (.NET)

Étapes suivantes

Pour en savoir plus sur l'utilisation de Powertools pour AWS, consultez les ressources suivantes :

- Outils électriques pour l'atelier AWS Lambda
- Modèles sans serveur qui utilisent Powertools pour AWS
- AWS objectif sans serveur bien conçu
- Création d'API sans serveur avec Powertools pour Lambda AWS

Gestion des flux de travail et des événements Lambda

Lorsque vous créez des applications sans serveur avec Lambda, vous avez souvent besoin de moyens pour orchestrer l'exécution des fonctions et gérer les événements. AWS propose plusieurs approches pour coordonner les fonctions d'événement Lambda :

- Fonctions durables Lambda pour une orchestration de flux de travail axée sur le code au sein de Lambda
- AWS Step Functions pour une orchestration visuelle du flux de travail entre plusieurs services
- Amazon EventBridge Scheduler et Amazon EventBridge pour les architectures et la planification axées sur les événements

Vous pouvez également intégrer ces approches ensemble. Par exemple, vous pouvez utiliser EventBridge Scheduler pour déclencher des fonctions durables ou des flux de travail Step Functions lorsque des événements spécifiques se produisent, ou configurer des flux de travail pour publier des événements sur EventBridge Scheduler à des points d'exécution définis. Les rubriques suivantes de cette section fournissent des informations supplémentaires sur la manière dont vous pouvez utiliser ces options d'orchestration.

Code-first orchestration avec fonctions durables

Les fonctions Lambda durables offrent une approche d'orchestration des flux de travail axée sur le code, vous permettant de créer des flux de travail dynamiques et de longue durée directement dans vos fonctions Lambda. Contrairement aux services d'orchestration externes, les fonctions durables maintiennent la logique de votre flux de travail dans le code, ce qui facilite la mise à jour, le test et la maintenance parallèlement à votre logique métier.

Les fonctions durables sont idéales lorsque vous avez besoin de :

- Utiliser des langages de programmation standard : définissez des flux de travail à l'aide de langages de programmation courants tels que JavaScript Python
- Long-running processus : exécutez des flux de travail pouvant durer jusqu'à un an, bien au-delà de la limite d'invocation par défaut de 15 minutes
- Développement simplifié : conservez la logique du flux de travail et la logique métier dans la même base de code pour faciliter la maintenance et les tests
- Cost-effective attente : interrompt l'exécution pendant les états d'attente sans consommer de ressources de calcul

- Built-in gestion des états : point de contrôle automatique et persistance des états sans configuration de stockage externe

Pour vous aider à choisir entre les fonctions durables et les Step Functions, voir Durable functions ou Step Functions.

Pour plus d'informations sur les fonctions durables, consultez la section Fonctions durables Lambda.

Orchestration de flux de travail avec Step Functions

AWS Step Functions est un service d'orchestration de flux de travail qui vous aide à coordonner plusieurs fonctions Lambda et AWS d'autres services dans des flux de travail structurés. Ces flux de travail peuvent maintenir l'état, gérer les erreurs grâce à des mécanismes de nouvelle tentative sophistiqués et traiter les données à grande échelle.

Step Functions propose deux types de flux de travail pour répondre aux différents besoins d'orchestration :

Flux de travail standard

: Idéal pour les flux de travail auditables de longue durée qui nécessitent une sémantique d'exécution unique. Les flux de travail standard peuvent s'exécuter pendant un an au maximum, fournissent un historique d'exécution détaillé et prennent en charge le débogage visuel. Ils conviennent aux processus comme l'exécution des commandes, les pipelines de traitement des données ou les tâches d'analytique en plusieurs étapes.

Flux de travail express

: Conçu pour les charges de travail de courte durée et à fréquence élevée avec une sémantique d'exécution au moins une fois. Les flux de travail express peuvent s'exécuter pendant jusqu'à cinq minutes et sont idéaux pour le traitement d'événements volumineux, les transformations de données de diffusion en continu ou les scénarios d'ingestion de données IoT. Ils offrent un débit plus élevé et un coût potentiellement inférieur par rapport aux flux de travail standard.

> **Note**
>
> Pour plus d'informations sur les types de flux de travail Step Functions, consultez Choix du type de flux de travail dans Step Functions.

Dans le cadre de ces flux de travail, Step Functions fournit deux types d'états Carte pour le traitement parallèle :

Inline Map

Traite les éléments d'un tableau JSON dans l'historique d'exécution du flux de travail parent. Inline Map prend en charge jusqu'à 40 itérations simultanées et convient aux petits jeux de données ou lorsque vous devez conserver tous les traitements dans une seule exécution. Pour plus d'informations, consultez Utilisation de l'état Map en mode Inline.

Plan distribué

Permet le traitement de charges de travail parallèles à grande échelle en itérant sur des jeux de données supérieurs à 256 Kio ou nécessitant plus de 40 itérations simultanées. Prenant en charge jusqu'à 10 000 exécutions parallèles de flux de travail enfants, Distributed Map excelle dans le traitement des données semi-structurées stockées dans Amazon S3, comme les fichiers JSON ou CSV, ce qui le rend idéal pour le traitement par lots et les opérations ETL. Pour plus d'informations, consultez Utilisation de l'état Map en mode Distributed.

En combinant ces types de flux de travail et les états Map, Step Functions fournit un ensemble d'outils flexible et puissant pour orchestrer des applications sans serveur complexes, qu'il s'agisse d'opérations à petite échelle ou de pipelines de traitement de données à grande échelle.

Pour commencer à utiliser Lambda avec Step Functions, consultez Orchestration de fonctions Lambda avec Step Functions.

Gestion des événements avec EventBridge et EventBridge planificateur

Amazon EventBridge est un service de bus d'événements qui vous aide à créer des architectures axées sur les événements. Il achemine les événements entre les AWS services, les applications intégrées et les applications SaaS (Software as a Service). EventBridge Le planificateur est un planificateur sans serveur. Avec EventBridge Scheduler, vous pouvez créer, exécuter et gérer des tâches à partir d'un service central, invoquer des fonctions Lambda selon un calendrier à l'aide d'expressions cron et rate, ou configurer des appels ponctuels.

Amazon EventBridge et EventBridge Scheduler vous aident à créer des architectures axées sur les événements avec Lambda. EventBridge achemine les événements entre les AWS services, les applications intégrées et les applications SaaS, tandis que EventBridge Scheduler fournit des fonctionnalités de planification spécifiques pour appeler les fonctions Lambda de manière récurrente ou ponctuelle.

Ces services fournissent plusieurs fonctionnalités clés pour travailler avec les fonctions Lambda :

- Créez des règles qui font correspondre les événements aux fonctions Lambda et les acheminent vers ces fonctions à l'aide de EventBridge
- Configurez des invocations de fonctions récurrentes à l'aide d'expressions cron et rate avec Scheduler EventBridge
- Configurer des invocations de fonction ponctuelles à des dates et heures spécifiques
- Définissez des fenêtres horaires flexibles et des politiques de nouvelle tentative pour les invocations planifiées

Pour plus d'informations, consultez Invoquer une fonction d'événement Lambda selon un calendrier.

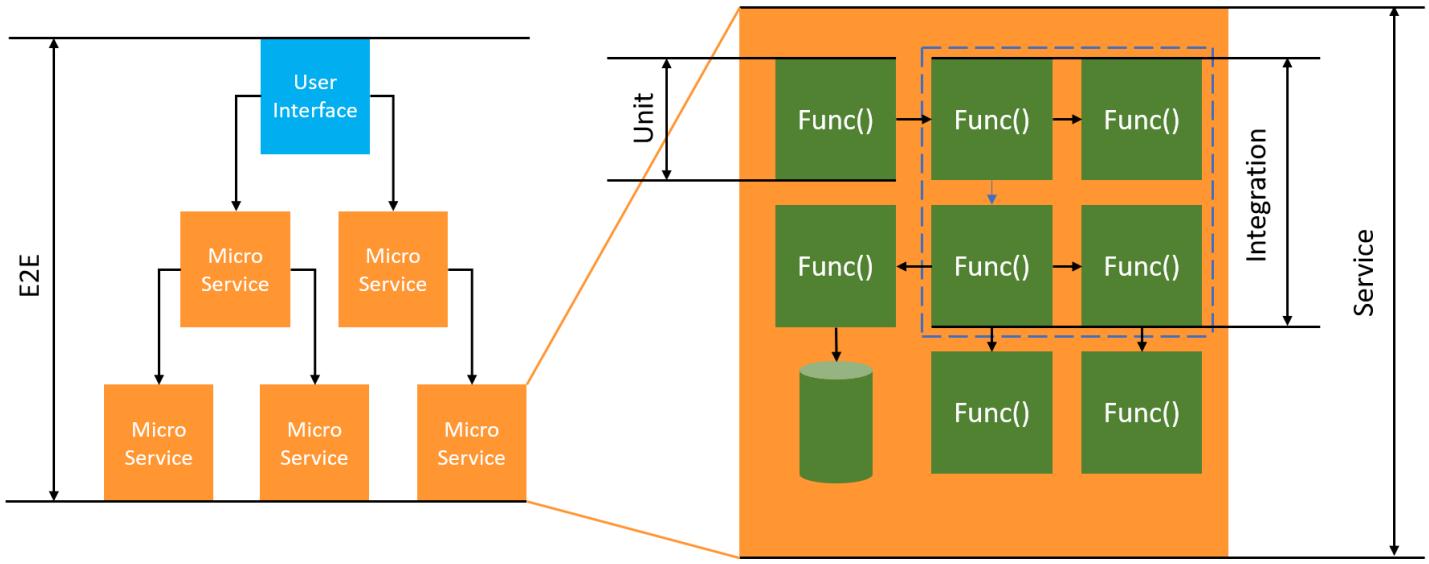
Commenter tester des fonctions et des applications sans serveur

Le test des fonctions sans serveur utilise des types et des techniques de test traditionnels, mais vous devez également envisager de tester les applications sans serveur dans leur ensemble. Cloud-based les tests fournissent la mesure la plus précise de la qualité de vos fonctions et de vos applications sans serveur.

Une architecture d’application sans serveur comprend des services gérés qui fournissent des fonctionnalités d’applications critiques par le biais d’appels d’API. C’est pourquoi votre cycle de développement doit inclure des tests automatisés qui vérifient la fonctionnalité lorsque votre fonction et vos services interagissent.

Si vous ne créez pas de tests basés sur le cloud, vous pouvez rencontrer des problèmes en raison des différences entre votre environnement local et l’environnement déployé. Votre processus d’intégration continue doit exécuter des tests sur une série de ressources allouées dans le cloud avant de promouvoir votre code vers l’environnement de déploiement suivant, comme l’assurance qualité, la mise en place ou la production.

Poursuivez la lecture de ce petit guide pour en savoir plus sur les stratégies de test pour les applications sans serveur, ou rendez-vous sur le référentiel Serverless Test Samples pour vous plonger dans des exemples pratiques, spécifiques au langage et à l’exécution que vous avez choisis.



Pour les tests sans serveur, vous pouvez toujours écrire des tests unitaires, d'intégration et de bout en bout.

- Tests unitaires : tests exécutés sur un bloc de code isolé. Par exemple, la vérification de la logique métier permettant de calculer les frais de livraison en fonction d'un article et d'une destination donnés.
- Tests d'intégration : tests impliquant au moins deux composants ou services qui interagissent, généralement dans un environnement cloud. Par exemple, la vérification d'une fonction traite les événements d'une file d'attente.
- End-to-end tests - Tests qui vérifient le comportement dans l'ensemble d'une application. Il s'agit par exemple de s'assurer que l'infrastructure est correctement mise en place et que les événements circulent entre les services comme prévu pour enregistrer la commande d'un client.

Résultats commerciaux ciblés

La mise en place des tests de solutions sans serveur peut prendre plus de temps. Vous devez vérifier les interactions entre les services basées sur les événements. Gardez ces raisons commerciales pratiques à l'esprit lorsque vous lisez ce guide :

- Améliorer la qualité de votre application
- Réduire le temps nécessaire à la création de fonctionnalités et à la correction des bogues

La qualité d'une application dépend du test de nombreux scénarios. Tenez compte de vos scénarios commerciaux et automatisez les tests pour les exécuter sur les services cloud. Cela améliore la qualité de votre candidature.

Les bogues et les problèmes de configuration coûtent moins cher lorsqu'ils sont détectés au début du cycle de développement. Les problèmes qui passent inaperçus jusqu'à la production nécessitent plus d'efforts et plus de personnel pour les résoudre.

Une bonne stratégie de test sans serveur améliore la qualité des logiciels et accélère les itérations. Il vérifie que vos fonctions et applications d'événements Lambda fonctionnent comme prévu dans le cloud.

Que faut-il tester ?

Nous recommandons une stratégie de test qui teste les comportements des services gérés, la configuration du cloud, les politiques de sécurité et l'intégration avec votre code. Les tests comportementaux, également appelés tests de boîte noire, vérifient qu'un système fonctionne comme prévu sans en connaître les composants internes.

- Exécutez des tests unitaires pour vérifier la logique métier au sein des fonctions Lambda.
- Vérifiez que les services intégrés sont réellement invoqués et que les paramètres d’entrée sont corrects.
- Vérifiez qu’un événement passe en revue tous les services attendus de bout en bout dans un flux de travail.

Dans l'architecture serveur traditionnelle, les équipes testent souvent uniquement le code qui s'exécute sur le serveur d'applications. Ils considèrent les autres composants, services ou dépendances comme externes et hors de portée.

Les applications sans serveur consistent en de petites unités de travail. Les exemples incluent les fonctions Lambda qui récupèrent des produits depuis une base de données, traitent des éléments d'une file d'attente ou redimensionnent une image stockée. Chaque composant s'exécute dans son propre environnement. Les équipes gèrent bon nombre de ces petites unités au sein d'une seule application.

Certaines fonctionnalités peuvent être entièrement gérées par des services gérés tels qu'Amazon S3, ou créées sans code personnalisé. Il n'est pas nécessaire de tester ces services gérés. Cependant, vous devez tester la manière dont votre code s'y intègre.

Comment tester le sans serveur

Vous savez probablement comment tester les applications déployées localement. Vous écrivez des tests par rapport au code sur votre bureau ou dans des conteneurs. Par exemple, vous pouvez appeler un service Web local, puis vérifier la réponse.

Les solutions sans serveur utilisent votre code de fonction et des services gérés basés sur le cloud, tels que les files d'attente, les bases de données, les bus d'événements et les systèmes de messagerie. Ces composants se connectent via une architecture axée sur les événements, dans laquelle les messages, appelés événements, circulent d'une ressource à l'autre. Certaines interactions sont synchrones, comme un service Web qui renvoie des résultats immédiatement.

D'autres sont asynchrones, comme le placement d'éléments dans une file d'attente ou le démarrage d'une étape du flux de travail. Votre stratégie de test doit couvrir les deux types et tester les interactions entre les services. Pour les interactions asynchrones, vous devrez peut-être détecter des effets secondaires dans les composants en aval qui ne sont pas immédiatement visibles.

Il n'est pas possible de répliquer complètement un environnement cloud en local. Cela inclut les files d'attente, les tables de base de données, les bus d'événements et les politiques de sécurité. Les différences entre les environnements locaux et cloud sont à l'origine de problèmes. Ces différences augmentent le temps nécessaire pour reproduire et corriger les bogues.

Dans les applications sans serveur, les composants existent entièrement dans le cloud. Des tests par rapport au code et aux services cloud sont nécessaires pour développer des fonctionnalités et corriger les bogues.

Techniques de test

Votre stratégie de test inclut probablement une combinaison de techniques. Vous utilisez des tests interactifs rapides pour déboguer les fonctions de la console. Vous rédigez des tests unitaires automatisés pour vérifier la logique métier. Vous vérifiez les appels vers des services externes à l'aide de simulacres. Vous pouvez également effectuer un test avec des émulateurs qui imitent un service.

- the section called “Tests dans le cloud”: Vous déployez l'infrastructure et le code à tester avec des services, des politiques de sécurité et des configurations réels. Cloud-based les tests fournissent la mesure la plus précise de la qualité de votre code.

Le débogage d'une fonction dans la console est un moyen rapide de la tester dans le cloud. Vous pouvez choisir parmi des exemples d'événements de test ou créer un événement personnalisé. Vous pouvez également partager les événements de test avec votre équipe via la console.

Pour automatiser les tests au cours du cycle de développement et de construction, effectuez des tests en dehors de la console. Consultez les sections de ce guide consacrées aux tests spécifiques aux langues pour connaître les stratégies d'automatisation.

- the section called "Tester avec des simulations": Les maquettes sont des objets de votre code qui simulent un service externe. Ils fournissent un comportement prédéfini pour vérifier les appels de service et les paramètres. Un faux est un simulacre qui utilise des raccourcis pour simplifier ou accélérer les tests. Par exemple, un faux objet d'accès aux données peut renvoyer des données depuis un entrepôt de données en mémoire. Les simulations peuvent simplifier les dépendances complexes, mais elles peuvent entraîner la création d'un plus grand nombre de simulations pour remplacer les dépendances imbriquées.
- the section called "Tester localement en utilisant AWS SAM INTERFACE DE LIGNE DE COMMANDE (CLI)": utilisez la AWS SAM CLI pour appeler localement des fonctions Lambda dans des conteneurs Docker qui utilisent le même environnement d'exécution que Lambda. AWS Vous pouvez tester la logique d'une fonction et le traitement des événements sans déploiement dans le cloud.
- the section called "Tester avec émulation": Utilisez l'LocalStack intégration dans VS Code pour émuler plusieurs AWS services localement afin de tester les intégrations de services.

Tests dans le cloud

Les tests dans le cloud sont utiles pour toutes les phases de test : tests unitaires, tests d'intégration et tests de bout en bout. Les tests exécutés sur du code et des services basés sur le cloud fournissent la mesure la plus précise de la qualité de votre code.

Un moyen simple d'exécuter une fonction Lambda dans le cloud consiste à effectuer un événement de test dans le. Console de gestion AWS Un événement de test est une entrée JSON pour votre fonction. Si votre fonction ne nécessite aucune entrée, l'événement peut être un document JSON vide`{}`. La console fournit des exemples d'événements pour de nombreuses intégrations de services. Vous pouvez partager des événements avec votre équipe pour faciliter les tests.

Découvrez comment déboguer un exemple de fonction dans la console.

> **Note**
>
> Bien que l'exécution de fonctions dans la console soit un moyen rapide de déboguer, l'automatisation de vos cycles de test est essentielle pour améliorer la qualité des applications et la vitesse de développement.

Des exemples d'automatisation des tests sont disponibles dans le référentiel Serverless Test Samples. La ligne de commande suivante exécute un exemple de test d'intégration Python automatique :

```
python -m pytest -s tests/integration -v
```

Bien que le test soit exécuté localement, il communique avec des ressources basées sur le cloud. Ces ressources ont été déployées à l'aide de l'outil de ligne de AWS SAM commande AWS Serverless Application Model et. Le code de test extrait d'abord les sorties de la pile déployée, telles que le point de terminaison de l'API, l'ARN de la fonction et le rôle de sécurité.

Il envoie ensuite une demande au point de terminaison de l'API. La réponse contient une liste de compartiments Amazon S3. Ce test s'exécute sur des ressources basées sur le cloud pour vérifier qu'elles sont déployées, sécurisées et fonctionnent.

```
========================== test session starts ==========================
      platform darwin -- Python 3.10.10, pytest-7.3.1, pluggy-1.0.0
      -- /Users/t/code/aws/serverless-test-samples/python-test-samples/apigw-lambda/
venv/bin/python
      cachedir: .pytest_cache
      rootdir: /Users/t/code/aws/serverless-test-samples/python-test-samples/apigw-
lambda
      plugins: mock-3.10.0
      collected 1 item


      tests/integration/test_api_gateway.py::TestApiGateway::test_api_gateway

      --> Stack outputs:

        HelloWorldApi
        = https://p7teqs3162.execute-api.us-east-2.amazonaws.com/Prod/hello/
        > API Gateway endpoint URL for Prod stage for Hello World function
```

```
        PythonTestDemo
        = arn:aws:lambda:us-east-2:123456789012:function:testing-apigw-lambda-
PythonTestDemo-iSij8evaTdxl
        > Hello World Lambda Function ARN

        PythonTestDemoIamRole
        = arn:aws:iam::123456789012:role/testing-apigw-lambda-PythonTestDemoRole-
IZELQQ9MG4HQ
        > Implicit IAM Role created for Hello World function

      --> Found API endpoint for "testing-apigw-lambda" stack...
      --> https://p7teqs3162.execute-api.us-east-2.amazonaws.com/Prod/hello/
      API Gateway response:
      amplify-dev-123456789-deployment|myapp-prod-p-loggingbucket-123456|s3-java-
bucket-123456789
      PASSED

      ========================= 1 passed in 1.53s =========================
```

Pour le développement d'applications natives cloud, les tests dans le cloud offrent les avantages suivants :

- Vous pouvez tester tous les services disponibles.
- Vous utilisez toujours les API de service et les valeurs de retour les plus récentes.
- Un environnement de test dans le cloud ressemble beaucoup à votre environnement de production.
- Les tests peuvent porter sur les politiques de sécurité, les quotas de service, les configurations et les paramètres spécifiques à l'infrastructure.
- Chaque développeur peut rapidement créer un ou plusieurs environnements de test dans le cloud.
- Les tests dans le cloud renforcent la certitude que votre code s'exécute correctement en production.

Les tests dans le cloud présentent certains inconvénients. Les déploiements dans le cloud prennent généralement plus de temps que les déploiements de postes de travail locaux.

Des outils tels que AWS Serverless Application Model (AWS SAM) Accelerate, le mode veille du AWS Cloud Development Kit (AWS CDK) et le SST (tiers) réduisent cette latence. Ces outils surveillent votre infrastructure et votre code, puis déploient automatiquement les mises à jour dans votre environnement cloud.

> **Note**
>
> Découvrez comment créer une infrastructure sous forme de code dans le Guide du développeur sans serveur pour en savoir plus sur AWS Serverless Application Model CloudFormation, et Cloud Development Kit AWS (AWS CDK).

Contrairement aux tests locaux, les tests dans le cloud utilisent des ressources susceptibles d'entraîner des coûts. Les environnements de test isolés peuvent ajouter du travail à vos DevOps équipes, en particulier dans les organisations appliquant des contrôles de comptes stricts. Malgré tout, le temps consacré aux développeurs pour configurer un environnement local complexe peut coûter plus cher que l'utilisation d'environnements cloud jetables conçus à l'aide des outils Infrastructure as Code.

Même en tenant compte de ces considérations, les tests dans le cloud restent le meilleur moyen de garantir la qualité de vos solutions sans serveur.

Tester avec des simulations

Les tests avec des simulations sont une technique qui consiste à créer des objets de remplacement dans votre code afin de simuler le comportement d'un service cloud.

Par exemple, vous pouvez écrire un test qui utilise une maquette du service Amazon S3. Le simulateur renvoie une réponse définie chaque fois que la CreateObjectméthode est appelée. Il n'appelle pas Amazon S3 ni aucun autre point de terminaison de service.

Les frameworks fictifs génèrent souvent des objets fictifs pour vous. Certains frameworks sont génériques. D'autres ciblent AWS les SDK, comme Moto, une bibliothèque Python permettant de simuler des services. AWS

Les objets fictifs sont différents des émulateurs. Les développeurs créent des maquettes dans le cadre du code de test. Les émulateurs sont des applications autonomes qui présentent les mêmes fonctionnalités que les systèmes qu'ils imitent.

Les avantages de l'utilisation de simulations incluent les avantages suivants :

- Les simulations peuvent simuler des services tiers qui échappent au contrôle de votre application, tels que les API et les fournisseurs de logiciels en tant que service (SaaS), sans qu'il soit nécessaire d'accéder directement à ces services.

- Les simulations sont utiles pour tester les conditions d’échec, en particulier lorsque ces conditions sont difficiles à simuler, comme dans le cas d’une panne de service.
- Une fois configurée, la simulation permet d’effectuer des tests locaux rapides.
- Les simulations peuvent fournir un comportement de substitution pour pratiquement n’importe quel type d’objet. Les stratégies de simulations peuvent donc couvrir une plus grande variété de services que les émulateurs.
- Lorsque de nouvelles fonctionnalités ou de nouveaux comportements sont disponibles, les tests simulés permettent de réagir plus rapidement. En utilisant un framework de simulation générique, vous pouvez simuler de nouvelles fonctionnalités dès que le AWS SDK mis à jour sera disponible.

Les tests simulés présentent les inconvénients suivants :

- Les simulations nécessitent généralement un effort d'installation et de configuration non négligeable, en particulier lorsqu'il s'agit de déterminer les valeurs de retour de différents services pour simuler correctement les réponses.
- Les simulations sont écrites, configurées et doivent être mises à jour par les développeurs, ce qui accroît leurs responsabilités.
- Vous devrez peut-être avoir accès au cloud pour comprendre les API et les valeurs de retour des services.
- Les simulations peuvent être difficiles à entretenir. Lorsque les signatures des API cloud simulées changent ou que les schémas de valeurs de retour évoluent, vous devez mettre à jour vos simulations. Les simulations nécessitent également des mises à jour si vous étendez la logique de votre application pour effectuer des appels vers de nouvelles API.
- Les tests utilisant des simulations peuvent réussir dans les environnements de bureau, mais échouer dans le cloud. Les résultats peuvent ne pas correspondre à l'API actuelle. La configuration du service et les quotas ne peuvent pas être testés.
- Les frameworks fictifs sont limités lorsqu'il s'agit de tester ou de détecter les limites de quotas ou de politiques de gestion des AWS identités et des accès (IAM). Bien que les simulations soient plus efficaces pour simuler l'échec de l'autorisation ou le dépassement d'un quota, les tests ne permettent pas de déterminer quel résultat se produit réellement dans un environnement de production.

Tester localement en utilisant AWS SAM INTERFACE DE LIGNE DE COMMANDE (CLI)

Utilisez AWS SAM CLI pour tester vos fonctions dans des conteneurs Docker en utilisant le même environnement d'exécution que AWS Lambda. Vous pouvez tester la logique d'une fonction et le traitement des événements localement sans déploiement dans le cloud. Si votre fonction fait des appels d'API à d'autres Services AWS, ces appels atteignent AWS des ressources réelles.

Les avantages des tests avec des conteneurs locaux incluent les suivants :

- Utilise des environnements AWS Lambda d'exécution pour des tests précis.
- Permet d'effectuer des itérations de développement local rapides sans déploiement dans le cloud.
- Prend en charge le débogage à l'aide d'outils de développement locaux familiers.

Les tests avec les conteneurs locaux présentent les limites suivantes :

- Service AWS les appels de votre fonction interagissent avec des AWS ressources réelles, ce qui peut entraîner des coûts et affecter les données de production.
- Nécessite que Docker soit installé et exécuté localement.

Tester avec émulation

Les émulateurs sont des applications exécutées localement qui imitent les AWS services en fournissant des API et des valeurs de retour similaires. LocalStack est un outil d'émulation populaire qui fournit un environnement de développement local complet pour tester les intégrations de services.

LocalStack est un émulateur AWS Cloud que vous pouvez utiliser pour tester des applications sans serveur localement. Vous pouvez tester les fonctions Lambda qui s'intègrent à des services tels que DynamoDB, Amazon S3 et Amazon SQS sans vous connecter à des services réels. AWS Vous pouvez l'utiliser LocalStack dans le AWS Toolkit for VS Code.

Les avantages des tests avec émulateurs sont les suivants :

- Les émulateurs peuvent aider à accélérer les itérations et les tests de développement locaux.
- Les émulateurs fournissent un environnement familier aux développeurs habitués à développer du code dans un environnement local. Par exemple, si vous êtes habitué au développement d'une application à n niveaux, vous pouvez avoir un moteur de base de données et un serveur Web, similaires à ceux exécutés en production, exécutés sur votre machine locale pour fournir une capacité de test rapide, locale et isolée.

- Les émulateurs ne nécessitent aucune modification de l'infrastructure cloud (tels que les comptes cloud des développeurs). Ils sont donc faciles à mettre en œuvre avec les modèles de test existants.
- Comme les émulateurs n'utilisent pas de AWS ressources réelles, vous n'aurez pas à payer de frais imprévus lorsque vous démarrez plusieurs services ou si vous laissez certaines ressources fonctionner pendant de longues périodes.

Les tests avec des émulateurs présentent les inconvénients suivants :

- Les émulateurs peuvent être difficiles à configurer et à reproduire, en particulier lorsqu'ils sont utilisés dans CI/CD des pipelines. Cela peut accroître la charge de travail du personnel informatique ou des développeurs qui gèrent leurs propres logiciels.
- Les fonctionnalités et les API émulées sont généralement en retard par rapport aux mises à jour des services. Cela peut entraîner des erreurs parce que le code testé ne correspond pas à l'API réelle, et entraver l'adoption de nouvelles fonctionnalités.
- Les émulateurs nécessitent une assistance, des mises à jour, des corrections de bogues et des améliorations de la parité des fonctions. La responsabilité en incombe à l'auteur de l'émulateur, qui peut être une société tierce.
- Les tests qui s'appuient sur des émulateurs peuvent fournir des résultats positifs localement, mais échouer dans le cloud en raison de politiques de sécurité de production, de configurations inter-services ou du dépassement des quotas Lambda.

Bonnes pratiques

Les sections suivantes fournissent des recommandations pour réussir les tests d'applications sans serveur.

Vous trouverez des exemples pratiques de tests et d'automatisation des tests dans le référentiel Serverless Test Samples.

Prioriser les tests dans le cloud

Les tests dans le cloud fournissent la couverture de test la plus fiable, la plus précise et la plus complète. La réalisation de tests dans le contexte du cloud permet de tester de manière exhaustive non seulement la logique métier, mais également les politiques de sécurité, les configurations de service, les quotas, ainsi que les signatures d'API et les valeurs de retour les plus récentes.

Structurer votre code pour le rendre testable

Simplifiez vos tests et vos fonctions Lambda en séparant Lambda-specific le code de votre logique métier principale.

Votre gestionnaire de fonctions Lambda doit être un adaptateur léger qui prend en charge les données des événements et ne transmet que les détails importants à votre ou vos méthodes de logique métier. Grâce à cette stratégie, vous pouvez réaliser des tests complets autour de votre logique métier sans vous soucier des Lambda-specific détails. Vos fonctions AWS Lambda ne devraient pas nécessiter la configuration d'un environnement complexe ou d'un grand nombre de dépendances pour créer et initialiser le composant testé.

D’une manière générale, vous devez écrire un gestionnaire qui extrait et valide les données des objets d’événement et de contexte entrants, puis envoie ces données aux méthodes qui exécutent votre logique métier.

Accélérer les boucles de rétroaction du développement

Il existe des outils et des techniques permettant d’accélérer les boucles de rétroaction du développement. Par exemple, AWS SAM Accelerate et le mode de surveillance AWS CDK réduisent tous deux le temps nécessaire à la mise à jour des environnements cloud.

Les exemples du référentiel GitHub Serverless Test Samples explorent certaines de ces techniques.

Nous vous recommandons également de créer et de tester les ressources cloud le plus tôt possible au cours du développement, et pas seulement après une vérification du contrôle du code source. Cette pratique permet d’accélérer l’exploration et l’expérimentation lors du développement de solutions. En outre, l’automatisation du déploiement à partir d’une machine de développement vous permet de découvrir plus rapidement les problèmes de configuration du cloud et de réduire les efforts inutiles liés aux mises à jour et aux processus de révision du code.

Se concentrer sur les tests d’intégration

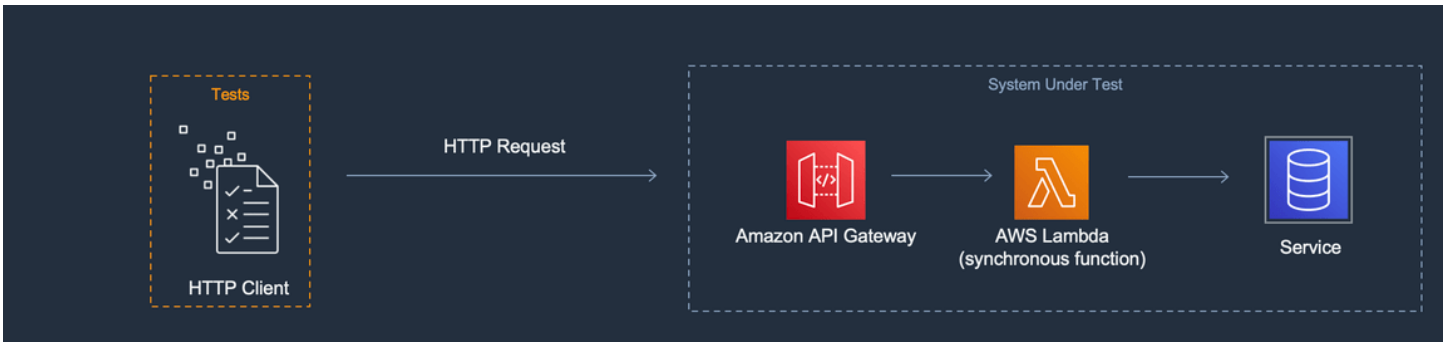
Lors de la création d’applications avec Lambda, il est recommandé de tester les composants ensemble.

Les tests exécutés sur deux composants architecturaux ou plus sont appelés tests d’intégration. L'objectif des tests d'intégration est de comprendre non seulement comment votre code s'exécute entre les composants, mais également le comportement de l'environnement hébergeant votre code.

End-to-end les tests sont des types spéciaux de tests d'intégration qui vérifient les comportements dans l'ensemble d'une application.

Pour créer des tests d'intégration, déployez votre application dans un environnement cloud. Cela peut être fait à partir d'un environnement local ou par le biais d'un CI/CD pipeline. Rédigez ensuite des tests pour exécuter le système sous test (SUT) et valider le comportement attendu.

Par exemple, le système testé pourrait être une application qui utilise API Gateway, Lambda et DynamoDB. Un test peut effectuer un appel HTTP synthétique vers un point de terminaison d'API Gateway et valider que la réponse contient la charge utile attendue. Ce test confirme que le code AWS Lambda est correct et que chaque service est correctement configuré pour traiter la demande, y compris les autorisations IAM entre eux. En outre, vous pouvez concevoir le test pour écrire des enregistrements de différentes tailles afin de vérifier que vos quotas de service, tels que la taille d'enregistrement maximale dans DynamoDB, sont correctement configurés.



Créer des environnements de test isolés

Les tests dans le cloud nécessitent généralement des environnements de développement isolés, de sorte que les tests, les données et les événements ne se chevauchent pas.

L'une des approches consiste à fournir à chaque développeur un AWS compte dédié. Cela permet d'éviter les conflits de dénomination des ressources qui peuvent survenir lorsque plusieurs développeurs travaillent dans une base de code partagée, tentent de déployer des ressources ou appellent une API.

Les processus de test automatisés doivent créer des ressources portant un nom unique pour chaque pile. Par exemple, vous pouvez configurer des scripts ou des fichiers de configuration TOML afin que les commandes AWS SAM CLI sam deploy ou sam sync spécifient automatiquement une pile avec un préfixe unique.

Dans certains cas, les développeurs partagent un AWS compte. Cela peut être dû au fait que votre stack contient des ressources coûteuses à exploiter, à provisionner et à configurer. Par exemple,

une base de données peut être partagée pour faciliter la configuration et l'amorçage appropriés des données

Si les développeurs partagent un compte, vous devez définir des limites afin d'identifier les propriétaires et d'éliminer les chevauchements. L'un des moyens d'y parvenir est de mettre des préfixes sur les noms de piles avec les identifiants d'utilisateurs des développeurs. Une autre approche populaire consiste à configurer des piles basées sur des branches de code. Avec les limites de branches, les environnements sont isolés, mais les développeurs peuvent toujours partager des ressources, telles qu'une base de données relationnelle. Cette approche est une bonne pratique lorsque les développeurs travaillent sur plusieurs branches à la fois.

Les tests dans le cloud sont utiles pour toutes les phases des tests, y compris les tests unitaires, les tests d'intégration et les tests de bout en bout. Il est essentiel de maintenir une isolation adéquate, mais vous souhaitez tout de même que votre environnement d'assurance qualité ressemble le plus possible à votre environnement de production. C'est pourquoi les équipes ajoutent des processus de contrôle des modifications pour les environnements d'assurance qualité.

Pour les environnements de pré-production et de production, les limites sont généralement définies au niveau du compte afin d'isoler les charges de travail de leurs bruyants voisins et de mettre en œuvre des contrôles de sécurité du moindre privilège pour protéger les données sensibles. Les charges de travail sont soumises à des quotas. Vous ne voulez pas que vos tests consomment les quotas alloués à la production (voisin bruyant) ou qu'ils aient accès aux données des clients. Les tests de charge constituent une autre activité que vous devez isoler de votre pile de production.

Dans tous les cas, les environnements doivent être configurés avec des alertes et des contrôles afin d'éviter des dépenses inutiles. Par exemple, vous pouvez limiter le type, le niveau ou la taille des ressources qui peuvent être créées, et configurer des alertes par e-mail lorsque les coûts estimés dépassent un seuil donné.

Utiliser des simulations pour isoler la logique métier

Les cadres simulés sont un outil précieux pour écrire des tests unitaires rapides. Ils sont particulièrement utiles lorsque les tests couvrent une logique interne complexe, tels que des calculs mathématiques ou financiers ou des simulations. Recherchez les tests unitaires qui comportent un grand nombre de cas de test ou de variations d'entrée, dans lesquels ces entrées ne modifient ni le modèle ni le contenu des appels vers d'autres services cloud.

Le code couvert par des tests unitaires avec des simulations doit également être couvert par des tests dans le cloud. Cela est recommandé, car un ordinateur portable de développeur ou un

environnement de machine de génération peuvent être configurés différemment d'un environnement de production dans le cloud. Par exemple, vos fonctions Lambda peuvent utiliser plus de mémoire ou de temps que ce qui est alloué lorsqu'elles sont exécutées avec certains paramètres d'entrée. Votre code peut également inclure des variables d'environnement qui ne sont pas configurées de la même manière (ou pas du tout), et les différences peuvent entraîner un comportement différent ou un échec du code.

L'avantage des simulations est moindre pour les tests d'intégration, car le niveau d'effort nécessaire à la mise en œuvre des simulations nécessaires augmente avec le nombre de points de connexion. End-to-end les tests ne doivent pas utiliser de simulations, car ces tests portent généralement sur des états et une logique complexe qui ne peuvent pas être facilement simulés avec des frameworks fictifs.

Enfin, évitez d'utiliser des services cloud simulés pour valider la bonne mise en œuvre des appels de service. Au lieu de cela, faites des appels de services dans le cloud pour valider le comportement, la configuration et la mise en œuvre fonctionnelle.

Utiliser les émulateurs avec parcimonie

Les émulateurs peuvent être pratiques dans certains cas d'utilisation, par exemple pour une équipe de développement disposant d'un accès Internet limité, peu fiable ou lent. Mais, dans la plupart des cas, choisissez d'utiliser les émulateurs avec parcimonie.

En évitant les émulateurs, vous pouvez créer et innover avec les fonctionnalités de service les plus récentes et les API les plus récentes. Vous n'êtes pas obligé d'attendre les versions des fournisseurs pour atteindre la parité des fonctionnalités. Vous réduisez vos dépenses initiales et permanentes d'achat et de configuration sur plusieurs systèmes de développement et machines de construction. De plus, vous évitez le problème selon lequel de nombreux services cloud ne disposent tout simplement pas d'émulateurs. Une stratégie de test qui repose sur l'émulation rend impossible l'utilisation de ces services (ce qui entraîne des solutions de contournement potentiellement plus coûteuses) ou produit du code et des configurations qui ne sont pas bien testés.

Lorsque vous utilisez l'émulation à des fins de test, vous devez tout de même effectuer des tests dans le cloud pour vérifier la configuration et tester les interactions avec les services cloud qui ne peuvent être simulés que dans un environnement émulé.

Défis liés aux tests locaux

Lorsque vous utilisez des émulateurs et des appels simulés pour effectuer des tests sur votre poste de travail local, vous risquez de rencontrer des incohérences au fur et à mesure que votre

code progresse d'un environnement à l'autre dans votre pipeline. CI/CD Les tests unitaires visant à valider la logique métier de votre application sur votre poste de travail risquent de ne pas tester avec précision les aspects critiques des services cloud.

Les exemples suivants présentent des cas à surveiller lors de tests locaux à l'aide de simulations et d'émulateurs :

Exemple : Event Function crée un compartiment S3

Si la logique d'une fonction Lambda dépend de la création d'un compartiment S3, un test complet devrait confirmer qu'Amazon S3 a été appelé et que le compartiment a été créé avec succès.

- Dans le cas d'un test simulé, vous pouvez simuler une réponse de réussite et éventuellement ajouter un scénario de test pour gérer une réponse d'échec.
- Dans un scénario de test d'émulation, l'CreateBucketAPI peut être appelée, mais vous devez savoir que l'identité à l'origine de l'appel local ne provient pas du service Lambda. L'identité d'appel ne joue pas un rôle de sécurité comme dans le cloud. C'est pourquoi une authentification par espace réservé est utilisée à la place, éventuellement avec un rôle plus permissif ou une identité d'utilisateur différente lorsqu'elle est exécutée dans le cloud.

Les configurations de simulation et d'émulation testent ce que fait la fonction Lambda si elle appelle Amazon S3 ; toutefois, ces tests ne vérifient pas que la fonction Lambda, telle que configurée, est capable de créer avec succès le compartiment Amazon S3. Vous devez vous assurer que le rôle attribué à la fonction dispose d'une politique de sécurité attachée qui autorise la fonction à effectuer l'action `s3:CreateBucket`. Dans le cas contraire, la fonction échoue probablement lorsqu'elle est déployée dans un environnement cloud.

Exemple : Event Function traite les messages d'une file d'attente Amazon SQS

Si une file d'attente Amazon SQS est la source d'une fonction Lambda, un test complet doit vérifier que la fonction Lambda est correctement invoquée lorsqu'un message est placé dans une file d'attente.

Les tests d'émulation et les tests fictifs sont généralement configurés pour exécuter directement le code de la fonction Lambda et pour simuler l'intégration Amazon SQS en transmettant une charge utile d'événement JSON (ou un objet désérialisé) comme entrée du gestionnaire de fonctions.

Les tests locaux qui simulent l'intégration Amazon SQS testent ce que fait la fonction Lambda lorsqu'elle est appelée par Amazon SQS avec une charge utile donnée, mais le test ne vérifie

pas qu'Amazon SQS appelle correctement la fonction Lambda lorsqu'elle est déployée dans un environnement cloud.

Voici quelques exemples de problèmes de configuration que vous pouvez rencontrer avec Amazon SQS et Lambda :

- Le délai de visibilité d'Amazon SQS est trop court, ce qui entraîne des invocations multiples alors qu'une seule était prévue.
- Le rôle d'exécution de la fonction Lambda n'autorise pas la lecture de messages depuis la file d'attente (via `sqs:ReceiveMessagesqs:DeleteMessage`, ou`sqs:GetQueueAttributes`).
- L'exemple d'événement transmis à la fonction Lambda dépasse le quota de taille de message Amazon SQS. Par conséquent, le test n'est pas valide, car Amazon SQS ne sera jamais en mesure d'envoyer un message de cette taille.

Comme le montrent ces exemples, les tests qui couvrent la logique métier mais pas les configurations entre les services cloud sont susceptibles de fournir des résultats peu fiables.

FAQ

J'ai une fonction Lambda qui effectue des calculs et renvoie un résultat sans appeler aucun autre service. Dois-je vraiment le tester dans le cloud ?

Oui. Les fonctions Lambda comportent des paramètres de configuration susceptibles de modifier le résultat du test. Tout le code de la fonction Lambda dépend des paramètres de délai d'attente et de mémoire, ce qui peut entraîner l'échec de la fonction si ces paramètres ne sont pas définis correctement.

Les politiques Lambda permettent également la journalisation des sorties standard sur Amazon. CloudWatch Même si votre code n'appelle pas CloudWatch directement, une autorisation est nécessaire pour activer la journalisation. Cette autorisation requise ne peut pas être simulée ou émulée avec précision.

Comment les tests dans le cloud peuvent-ils faciliter les tests unitaires ? S'il se trouve dans le cloud et qu'il se connecte à d'autres ressources, n'est-ce pas un test d'intégration ?

Nous définissons les tests unitaires comme des tests qui opèrent sur des composants architecturaux de manière isolée, mais cela n'empêche pas les tests d'inclure des composants susceptibles d'appeler d'autres services ou d'utiliser certaines communications réseau.

De nombreuses applications sans serveur possèdent des composants architecturaux qui peuvent être testés de manière isolée, même dans le cloud. Un exemple est celui d'une fonction Lambda qui prend une entrée, traite les données et envoie un message à une file d'attente Amazon SQS. Un test unitaire de cette fonction devrait permettre de vérifier si les valeurs d'entrée entraînent la présence de certaines valeurs dans le message en file d'attente.

Prenons l'exemple d'un test écrit en utilisant le modèle organiser, agir, affirmer :

- Organiser : allouez des ressources (une file d'attente pour recevoir des messages et la fonction en cours de test).
- Agir : appelez la fonction en cours de test.
- Affirmer : récupérez le message envoyé par la fonction et validez la sortie.

Une approche de test simulé consiste à simuler la file d'attente avec un objet simulé en cours de traitement et à créer une instance en cours de traitement de la classe ou du module contenant le code de la fonction Lambda. Pendant la phase d'assertion, le message en file d'attente est récupéré dans l'objet simulé.

Dans une approche basée sur le cloud, le test crée une file d'attente Amazon SQS pour les besoins du test et déploie la fonction Lambda avec des variables d'environnement configurées pour utiliser la file d'attente Amazon SQS isolée comme destination de sortie. Après avoir exécuté la fonction Lambda, le test récupère le message dans la file d'attente Amazon SQS.

Le test basé sur le cloud exécuterait le même code, affirmerait le même comportement et validerait l'exactitude fonctionnelle de l'application. Cependant, cela aurait l'avantage supplémentaire de pouvoir valider les paramètres de la fonction Lambda : le rôle IAM, les politiques IAM, le délai d'expiration et les paramètres de mémoire de la fonction.

Prochaines étapes et ressources

Les ressources suivantes vous permettront d'en savoir plus et de découvrir des exemples pratiques de tests.

Exemples d'implémentations

Le référentiel Serverless Test Samples GitHub contient des exemples concrets de tests qui suivent les modèles et les meilleures pratiques décrits dans ce guide. Le référentiel contient des exemples de code et des descriptions guidées des processus de simulation, d'émulation et de test dans le cloud

décrits dans les sections précédentes. Utilisez ce référentiel pour vous familiariser avec les derniers conseils de test sans serveur publiés par AWS.

Suggestions de lecture

Visitez Serverless Land pour accéder aux derniers blogs, vidéos et formations sur les technologies AWS sans serveur.

Il est également recommandé de lire les articles de AWS blog suivants :

- Accélérer le développement sans serveur avec AWS SAM Accelerate (article de AWS blog)
- Accroître la vitesse de développement avec CDK Watch (article de AWS blog)
- Simulation d'intégrations de services avec AWS Step Functions Local (AWS article de blog)
- Commencer à tester des applications sans serveur (article de AWS blog)

Outils

- AWS SAM — Tester et déboguer des applications sans serveur
- AWS SAM — Intégration aux tests automatisés
- Lambda : test des fonctions Lambda dans la console Lambda

Gestion des autorisations dans AWS Lambda

Vous pouvez utiliser Gestion des identités et des accès AWS (IAM) pour gérer les autorisations dans AWS Lambda. Il existe deux catégories principales d'autorisations que vous devez prendre en compte lorsque vous travaillez avec les fonctions d'événement Lambda :

- Autorisations dont vos fonctions Lambda ont besoin pour effectuer des actions d'API et accéder à d'autres ressources AWS
- Autorisations dont AWS les autres utilisateurs et entités ont besoin pour accéder à vos fonctions Lambda. Pour plus d’informations, consultez the section called “Autorisations d’accès (autorisations permettant à d’autres entités d’accéder à vos fonctions)”.

Les fonctions Lambda ont souvent besoin d'accéder à d'autres AWS ressources et d'effectuer diverses opérations d'API sur ces ressources. Par exemple, vous pouvez disposer d’une fonction Lambda qui répond à un événement en mettant à jour les entrées d’une base de données Amazon

DynamoDB. Dans ce cas, votre fonction a besoin d'autorisations pour accéder à la base de données, ainsi que d'autorisations pour mettre ou mettre à jour des éléments dans cette base de données.

Vous définissez les autorisations dont votre fonction Lambda a besoin dans un rôle IAM spécial appelé rôle d'exécution. Dans ce rôle, vous pouvez associer une politique qui définit toutes les autorisations dont votre fonction a besoin pour accéder à d'autres AWS ressources et lire des sources d'événements. Chaque fonction Lambda doit avoir un rôle d'exécution. Au minimum, votre rôle d'exécution doit avoir accès à Amazon CloudWatch car les fonctions Lambda se connectent par défaut à CloudWatch Logs. Vous pouvez associer la politique gérée par `AWSLambdaBasicExecutionRole` à votre rôle d'exécution pour répondre à cette exigence.

Pour autoriser d'autres Comptes AWS organisations et services à accéder à vos ressources Lambda, plusieurs options s'offrent à vous :

- Vous pouvez utiliser des politiques basées sur l'identité pour autoriser d'autres utilisateurs à accéder à vos ressources Lambda. Identity-based les politiques peuvent s'appliquer directement aux utilisateurs ou aux groupes et rôles associés à un utilisateur.
- Vous pouvez utiliser des politiques basées sur les ressources pour accorder à d'autres comptes et Services AWS autorisations l'accès à vos ressources Lambda. Lorsqu'un utilisateur essaie d'accéder à une ressource Lambda, Lambda prend en compte à la fois les stratégies basées sur l'identité appartenant à l'utilisateur et la stratégie basée sur une ressource appartenant aux ressources. Lorsqu'un AWS service tel qu'Amazon Simple Storage Service (Amazon S3) appelle votre fonction Lambda, Lambda ne prend en compte que la politique basée sur les ressources.
- Vous pouvez utiliser un modèle de contrôle d'accès par attributs (ABAC) pour contrôler l'accès à vos fonctions Lambda. Avec ABAC, vous pouvez attacher des balises à une fonction Lambda, les transmettre dans certaines requêtes d'API ou les attacher au principal IAM qui effectue la requête. Spécifiez les mêmes balises dans l'élément condition d'une politique IAM pour contrôler l'accès aux fonctions.

Dans AWS, il est recommandé d'accorder uniquement les autorisations requises pour effectuer une tâche (autorisations du moindre privilège). Pour implémenter cela dans Lambda, nous vous recommandons de commencer par une politique gérée par AWS. Vous pouvez utiliser ces stratégies gérées telles quelles ou comme point de départ pour créer des stratégies plus restrictives.

Pour vous aider à optimiser vos autorisations d'accès avec le moindre privilège, Lambda fournit des conditions supplémentaires que vous pouvez inclure dans vos politiques. Pour plus d'informations, consultez the section called "Ressources et conditions".

Pour de plus amples informations sur IAM, consultez le Guide de l'utilisateur IAM.

Définition des autorisations de la fonction d'événement Lambda avec un rôle d'exécution

Le rôle d'exécution d'une fonction d'événement Lambda est un rôle Gestion des identités et des accès AWS (IAM) qui accorde à la fonction l'autorisation d'accès Services AWS et de ressources. Par exemple, vous pouvez créer un rôle d'exécution autorisé à envoyer des journaux à Amazon CloudWatch et à y télécharger des données de suivi AWS X-Ray. Cette page fournit des informations sur la façon de créer, d'afficher et de gérer le rôle d'exécution d'une fonction Lambda.

Lambda assume automatiquement votre rôle d'exécution lorsque vous appelez votre fonction. Vous devez éviter d'appeler `sts:AssumeRole` manuellement afin d'assumer le rôle d'exécution dans votre code de fonction. Si votre cas d'utilisation nécessite que le rôle soit assumé par lui-même, vous devez inclure le rôle lui-même en tant que principal approuvé dans la politique d'approbation de votre rôle. Pour en savoir plus sur la procédure de modification d'une politique d'approbation des rôles, consultez Modification d'une politique d'approbation de rôle (console)dans le Guide de l'utilisateur IAM.

Pour que Lambda assume correctement votre rôle d'exécution, la politique de confiance du rôle doit spécifier le principal de service Lambda (`lambda.amazonaws.com`) comme un service de confiance.

Rubriques

- Création d'un rôle d'exécution dans la console IAM
- Création et gestion des rôles à l'aide du AWS CLI
- Accorder un accès assorti d'un privilège minimum à votre rôle d'exécution Lambda
- Affichage et mise à jour des autorisations dans le rôle d'exécution
- Utilisation de politiques AWS gérées dans le rôle d'exécution
- Utilisation de l'ARN de la fonction source pour contrôler le comportement d'accès aux fonctions

Création d'un rôle d'exécution dans la console IAM

Par défaut, Lambda crée un rôle d'exécution avec des autorisations minimales lorsque vous créez une fonction dans la console Lambda. Plus précisément, ce rôle d'exécution inclut la politique `AWSLambdaBasicExecutionRole` gérée, qui donne à votre fonction les autorisations de base pour consigner des événements sur Amazon CloudWatch Logs. Vous pouvez sélectionner Créer un rôle par défaut dans la section Autorisations.

Vous pouvez choisir un rôle existant en sélectionnant Utiliser un autre rôle dans la section Autorisations. Si votre fonction Lambda a besoin d'autorisations supplémentaires pour effectuer des tâches telles que la mise à jour des entrées dans une base de données Amazon DynamoDB en réponse à des événements, vous pouvez créer un rôle d'exécution personnalisé avec les autorisations nécessaires. Pour ce faire, sélectionnez Utiliser un autre rôle dans la section Autorisations, qui ouvre un tiroir dans lequel vous pouvez personnaliser vos autorisations.

> **Note**
>
> Si le gestionnaire de rôles est activé dans votre compte, la console Lambda vous associe un rôle d'exécution. Pour personnaliser les autorisations, créez votre fonction, puis modifiez les autorisations de la fonction pour sélectionner un autre rôle ou personnaliser le rôle associé. Pour plus d'informations, voir Création automatique de rôles avec le gestionnaire de rôles dans le guide de l'utilisateur IAM.

Pour configurer un rôle d'exécution depuis la console

1. Entrez un nom de rôle dans la section Détails du rôle.
2. Dans la section Stratégie, sélectionnez Utiliser la politique existante.
3. Sélectionnez les politiques AWS gérées que vous souhaitez associer à votre rôle. Par exemple, si votre fonction doit accéder à DynamoDB, sélectionnez AWSLambdaDynamoDBExecutionRolela politique gérée.
4. Choisissez Créer un rôle.

Lorsque vous créez une fonction dans la console Lambda, vous pouvez également associer à la fonction n'importe quel rôle d'exécution que vous avez créé précédemment. Si vous souhaitez associer un nouveau rôle d'exécution à une fonction existante, suivez les étapes décrites dans Mettre à jour le rôle d'exécution d'une fonction.

Création et gestion des rôles à l'aide du AWS CLI

Pour créer un rôle d'exécution avec le AWS Command Line Interface (AWS CLI), utilisez la create-role commande. Lorsque vous utilisez cette commande, vous pouvez préciser la politique d'approbation en ligne. La politique d'approbation d'un rôle accorde aux principaux spécifiés l'autorisation d'assumer le rôle. Dans l'exemple suivant, vous accordez au service Lambda

l'autorisation principale d'assumer votre rôle. Notez que les exigences relatives à l'exclusion des guillemets dans la chaîne JSON peuvent varier en fonction de votre shell.

```
aws iam create-role \
  --role-name lambda-ex \
  --assume-role-policy-document '{"Version": "2012-10-17",       "Statement":
 [{ "Effect": "Allow", "Principal": {"Service": "lambda.amazonaws.com"}, "Action":
 "sts:AssumeRole"}]}'
```

Vous pouvez également définir la politique d'approbation pour le rôle à l'aide d'un fichier JSON séparé. Dans l'exemple suivant, le fichier `trust-policy.json` se trouve dans le répertoire actuel.

Example trust-policy.json

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

```
aws iam create-role \
  --role-name lambda-ex \
  --assume-role-policy-document file://trust-policy.json
```

Pour ajouter des autorisations au rôle, utilisez la commande attach-policy-to-role. La commande suivante ajoute la politique gérée `AWSLambdaBasicExecutionRole` au rôle d'exécution `lambda-ex`.

```
aws iam attach-role-policy --role-name lambda-ex --policy-arn arn:aws:iam::aws:policy/
service-role/AWSLambdaBasicExecutionRole
```

Après avoir créé votre rôle d'exécution, attachez-le à votre fonction. Lorsque vous créez une fonction dans la console Lambda, vous pouvez attacher n'importe quel rôle d'exécution précédemment créé à la fonction. Si vous souhaitez attacher un nouveau rôle d'exécution à une fonction existante, suivez les étapes décrites dans the section called "Mise à jour du rôle d'exécution d'une fonction".

Accorder un accès assorti d'un privilège minimum à votre rôle d'exécution Lambda

Lorsque vous créez pour la première fois un rôle IAM pour votre fonction Lambda pendant la phase de développement, il peut arriver que vous accordiez des autorisations au-delà de ce que est nécessaire. Avant de publier votre fonction dans l'environnement de production, une bonne pratique consiste à ajuster la stratégie de manière à inclure uniquement les autorisations requises. Pour plus d'informations, consultez la section Appliquer les autorisations de moindre privilège dans le Guide de l'utilisateur IAM.

Utilisez IAM Access Analyzer pour identifier les autorisations requises pour la stratégie de rôle d'exécution IAM. IAM Access Analyzer examine vos AWS CloudTrail journaux pendant la période que vous spécifiez et génère un modèle de politique avec uniquement les autorisations utilisées par la fonction pendant cette période. Vous pouvez utiliser le modèle pour créer une stratégie gérée avec des autorisations affinées, puis l'attacher au rôle IAM. Ainsi, vous n'accordez que les autorisations dont le rôle a besoin pour interagir avec les AWS ressources correspondant à votre cas d'utilisation spécifique.

Pour plus d'informations, consultez la section Générer des politiques en fonction de l'activité d'accès dans le guide de l'utilisateur IAM.

Affichage et mise à jour des autorisations dans le rôle d'exécution

Cette rubrique explique comment afficher et mettre à jour le rôle d'exécution de votre fonction.

Rubriques

- Affichage du rôle d'exécution d'une fonction
- Mise à jour du rôle d'exécution d'une fonction

Affichage du rôle d'exécution d'une fonction

Pour afficher le rôle d'exécution d'une fonction, utilisez la console Lambda.

Pour afficher le rôle d'exécution d'une fonction (console)

1. Ouvrez la page Event Functions de la console Lambda.

2. Choisissez le nom d'une fonction.
3. Choisissez Configuration (Configuration), puis Permissions (Autorisations).
4. Sous Rôle d'exécution, vous pouvez afficher le rôle actuellement utilisé comme rôle d'exécution de la fonction. Par souci de commodité, vous pouvez consulter toutes les ressources et actions auxquelles la fonction peut accéder dans la section Synthèse des ressources. Vous pouvez également choisir un service dans la liste déroulante pour afficher toutes les autorisations associées à ce service.

Mise à jour du rôle d'exécution d'une fonction

À tout moment, vous pouvez ajouter ou supprimer des autorisations à partir du rôle d'exécution d'une fonction ou configurer votre fonction afin d'utiliser un autre rôle. Si votre fonction a besoin d'accéder à d'autres services ou ressources, vous devez ajouter les autorisations nécessaires au rôle d'exécution.

Lorsque vous ajoutez des autorisations à votre fonction, modifiez légèrement son code ou sa configuration. Cela force l'arrêt et le remplacement des instances en cours d'exécution de votre fonction, qui ont des informations d'identification obsolètes.

Pour mettre à jour le rôle d'exécution d'une fonction, vous pouvez utiliser la console Lambda.

Pour mettre à jour le rôle d'exécution d'une fonction (console)

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez le nom d'une fonction.
3. Choisissez Configuration (Configuration), puis Permissions (Autorisations).
4. Sous Rôle d'exécution, choisissez Modifier.
5. Si vous souhaitez mettre à jour votre fonction pour utiliser un autre rôle en tant que rôle d'exécution, choisissez le nouveau rôle dans le menu déroulant sous Rôle existant.

> **Note**
>
> Si vous souhaitez mettre à jour les autorisations au sein d'un rôle d'exécution existant, vous ne pouvez le faire que dans la console Gestion des identités et des accès AWS (IAM).

Si vous souhaitez créer un nouveau rôle à utiliser comme rôle d'exécution, choisissez Créer un nouveau rôle à partir de modèles de AWS politique sous Rôle d'exécution. Saisissez ensuite le nom de votre nouveau rôle sous Nom du rôle et spécifiez les politiques que vous souhaitez attacher au nouveau rôle sous Modèles de stratégies.

6. Cliquez sur Enregistrer.

Utilisation de politiques AWS gérées dans le rôle d'exécution

Les politiques AWS gérées suivantes fournissent les autorisations requises pour utiliser les fonctionnalités Lambda.

Modification	Description	Date
AWSLambdaMSKExecutionRôle — Lambda a ajouté l'autorisation Kafka : DescribeCluster V2 à cette politique.	`AWSLambdaMSKExecutionRole` accorde les autorisations nécessaires pour lire et accéder aux enregistrements d'un cluster Amazon Managed Streaming for Apache Kafka (Amazon MSK), gérer les interfaces réseau élastiques (ENIs) et écrire dans les journaux. CloudWatch	17 juin 2022
AWSLambdaBasicExecutionRole— Lambda a commencé à suivre les modifications apportées à cette politique.	`AWSLambdaBasicExecutionRole` accorde des autorisations pour charger les journaux sur CloudWatch.	14 février 2022
AWSLambdaDynamoDBExecution Role — Lambda a commencé à suivre les modifications apportées à cette politique.	`AWSLambdaDynamoDBExecutionRole` accorde l'autorisation de lire les enregistrements d'un flux	14 février 2022

Modification	Description	Date
	Amazon DynamoDB et d'écrire dans Logs. CloudWatch	
AWSLambdaKinesisExecutionRole— Lambda a commencé à suivre les modifications apportées à cette politique.	`AWSLambdaKinesisExecutionRole` accorde l'autorisation de lire les événements d'un flux de données Amazon Kinesis et d'écrire dans Logs. CloudWatch	14 février 2022
AWSLambdaMSKExecutionRôle — Lambda a commencé à suivre les modifications apportées à cette politique.	`AWSLambdaMSKExecutionRole` accorde les autorisations nécessaires pour lire et accéder aux enregistrements d'un cluster Amazon Managed Streaming for Apache Kafka (Amazon MSK), gérer les interfaces réseau élastiques (ENIs) et écrire dans les journaux. CloudWatch	14 février 2022
AWSLambdaSQSQueueExecutionRole— Lambda a commencé à suivre les modifications apportées à cette politique.	`AWSLambdaSQSQueueExecutionRole` accorde l'autorisation de lire un message depuis une file d'attente Amazon Simple Queue Service (Amazon SQS) et d'écrire dans Logs. CloudWatch	14 février 2022

Modification	Description	Date
AWSLambdaVPCAccessExecutionRole— Lambda a commencé à suivre les modifications apportées à cette politique.	`AWSLambdaVPCAccessExecutionRole` accorde des autorisations pour gérer ENIs au sein d'un Amazon VPC et écrire dans Logs. CloudWatch	14 février 2022
AWSXRayDaemonWriteAccess— Lambda a commencé à suivre les modifications apportées à cette politique.	`AWSXRayDaemonWriteAccess` accorde des autorisations pour charger des données de suivi vers X-Ray.	14 février 2022
CloudWatchLambdaInsightsExecutionRolePolicy— Lambda a commencé à suivre les modifications apportées à cette politique.	`CloudWatchLambdaInsightsExecutionRolePolicy` accorde l'autorisation d'écrire des métriques d'exécution dans CloudWatch Lambda Insights.	14 février 2022
AmazonS3 — ObjectLambdaExecutionRolePolicy Lambda a commencé à suivre les modifications apportées à cette politique.	`AmazonS3ObjectLambdaExecutionRolePolicy` accorde les autorisations nécessaires pour interagir avec l'objet Lambda d'Amazon Simple Storage Service (Amazon S3) et pour écrire dans Logs. CloudWatch	14 février 2022

Pour certaines fonctionnalités, la console Lambda tente d'ajouter les autorisations manquantes au rôle d'exécution dans une stratégie gérée par le client. Ces stratégies peuvent être excessivement nombreuses. Afin d'éviter la création de stratégies supplémentaires, ajoutez les stratégies gérées AWS pertinentes au rôle d'exécution avant d'activer les fonctions.

Lorsque vous utilisez un mappage de source d'événement pour appeler votre fonction, Lambda utilise le rôle d'exécution pour lire les données d'événement. Par exemple, un mappage de source d'événement pour Kinesis lit les événements d'un flux de données et les envoie à votre fonction par lots.

Lorsqu'un service endosse un rôle dans votre compte, vous pouvez inclure les clés de contexte de condition globale `aws:SourceAccount` et `aws:SourceArn` dans votre politique d'approbation des rôles afin de limiter l'accès au rôle aux seules demandes générées par les ressources attendues. Pour plus d'informations, consultez Prévention du problème de l'adjoint confus entre services pour AWS Security Token Service.

Outre les politiques AWS gérées, la console Lambda fournit des modèles permettant de créer une politique personnalisée avec des autorisations pour des cas d'utilisation supplémentaires. Lorsque vous créez une fonction dans la console Lambda, vous pouvez choisir de créer un nouveau rôle d'exécution doté des autorisations d'un ou plusieurs modèles. Ces modèles s'appliquent également automatiquement lorsque vous créez une fonction à partir d'un plan ou lorsque vous configurez les options qui nécessitent l'accès à d'autres services. Des exemples de modèles sont disponibles dans le GitHubréférentiel de ce guide.

Utilisation de l'ARN de la fonction source pour contrôler le comportement d'accès aux fonctions

Il est courant que le code de votre fonction d'événement Lambda envoie des demandes d'API à d'autres personnes. Services AWS Pour effectuer ces requêtes, Lambda génère un ensemble éphémère d'informations d'identification en assumant le rôle d'exécution de votre fonction. Ces informations d'identification sont disponibles en tant que variables d'environnement lors de l'appel de votre fonction. Lorsque vous travaillez avec des kits SDK AWS , vous n'avez pas besoin de fournir des informations d'identification pour le kit SDK directement dans le code. Par défaut, la chaîne de fournisseurs d'informations d'identification vérifie séquentiellement chaque endroit où vous pouvez définir des informations d'identification et sélectionne le premier disponible, généralement les variables d'environnement (`AWS_ACCESS_KEY_ID`, `AWS_SECRET_ACCESS_KEY` et `AWS_SESSION_TOKEN`).

Lambda injecte l'ARN de la fonction source dans le contexte des informations d'identification si la demande est une demande d' AWS API provenant de votre environnement d'exécution. Lambda injecte également l'ARN de la fonction source pour les demandes d'API AWS suivantes que Lambda effectue en votre nom en dehors de votre environnement d'exécution :

Service	Action	Raison
CloudWatch Journaux	`CreateLogGroup` , `CreateLogStream` , `PutLogEvents`	Pour stocker les journaux dans un groupe de CloudWatch journaux
X-Ray	`PutTraceSegments`	Pour envoyer des données de suivi à X-Ray
Amazon EFS	`ClientMount`	Pour connecter votre fonction à un système de fichiers Amazon Elastic File System (Amazon EFS)

Les autres appels d' AWS API que Lambda effectue en dehors de votre environnement d'exécution en votre nom en utilisant le même rôle d'exécution ne contiennent pas l'ARN de la fonction source. Voici des exemples de tels appels d'API en dehors de l'environnement d'exécution :

- Appelle to AWS Key Management Service (AWS KMS) pour chiffrer et déchiffrer automatiquement vos variables d'environnement.
- Appels à Amazon Elastic Compute Cloud (Amazon EC2) pour créer des interfaces réseau élastiques (ENI) pour une fonction. VPC-enabled
- Appels Services AWS, tels qu'Amazon Simple Queue Service (Amazon SQS), pour lire à partir d'une source d'événements configurée en tant que mappage de sources d'événements.

Avec l'ARN de la fonction source dans le contexte des informations d'identification, vous pouvez vérifier si un appel à votre ressource provient du code d'une fonction Lambda spécifique. Pour vérifier cela, utilisez le clé de condition `lambda:SourceFunctionArn` dans une politique IAM basée sur l'identité ou politique de contrôle des services (SCP).

> **Note**
>
> Vous ne pouvez pas utiliser l'élément `lambda:SourceFunctionArn` dans les politiques basées sur les ressources.

À l'aide de cette clé de condition dans vos politiques basées sur l'identité ou SCP, vous pouvez implémenter des contrôles de sécurité pour les actions d'API que votre code de fonction fait à d'autres Services AWS. Cela comporte quelques applications de sécurité clés, telles que l'identification de la source d'une fuite d'informations d'identification.

> **Note**
>
> La clé de condition `lambda:SourceFunctionArn` est différente des clés de condition `lambda:FunctionArn` et `aws:SourceArn`. Le clé de condition `lambda:FunctionArn` s'applique uniquement aux Mappages de sources d'événement et aide à définir les fonctions que votre source d'événement peut invoquer. La clé de `aws:SourceArn` condition s'applique uniquement aux politiques dans lesquelles votre fonction Lambda est la ressource cible et permet de définir quelles autres Services AWS ressources peuvent invoquer cette fonction. La clé de `lambda:SourceFunctionArn` condition peut s'appliquer à n'importe quelle politique basée sur l'identité ou à tout SCP afin de définir les fonctions Lambda spécifiques autorisées à effectuer des appels d' AWS API spécifiques vers d'autres ressources.

Pour utiliser `lambda:SourceFunctionArn` dans votre stratégie, incluez-la en tant que condition dans l'un des Opérateurs de condition ARN. La valeur de la clé doit être un ARN valide.

Par exemple, supposons que votre code de fonction Lambda émette un appel `s3:PutObject` qui cible un compartiment Amazon S3 spécifique. Vous pouvez vouloir n'autoriser qu'une fonction Lambda spécifique à avoir un accès `s3:PutObject` à ce compartiment. Dans ce cas, le rôle d'exécution de votre fonction doit être associé à une stratégie qui ressemble à ceci :

Example politique accordant à une fonction événementielle spécifique l'accès à une ressource Amazon S3

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ExampleSourceFunctionArn",
            "Effect": "Allow",
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::lambda_bucket/*",
```

```
            "Condition": {
                "ArnEquals": {
                    "lambda:SourceFunctionArn": "arn:aws:lambda:us-
east-1:123456789012:function:source_lambda"
                }
            }
        }
    ]
}
```

Cette politique permet uniquement un accès `s3:PutObject` si la source est la fonction Lambda avec ARN `arn:aws:lambda:us-east-1:123456789012:function:source_lambda`. Cette politique n'autorise pas un accès `s3:PutObject` à une autre identité d'appel. C'est le cas même si une fonction ou une entité différente émet un appel `s3:PutObject` avec le même rôle d'exécution.

> **Note**
>
> La clé de condition `lambda:SourceFunctionARN` ne prend pas en charge les versions des fonctions Lambda ni les alias de fonction. Si vous utilisez l'ARN pour une version ou un alias de fonction en particulier, votre fonction n'est pas autorisée à effectuer l'action que vous spécifiez. Veillez à utiliser l'ARN non qualifié pour votre fonction sans suffixe de version ou d'alias.

Vous pouvez également utiliser `lambda:SourceFunctionArn` dans les SCP. Supposons, par exemple, que vous souhaitiez limiter l'accès à votre compartiment à un code de fonction Lambda unique ou à des appels issus d'un cloud privé virtuel (VPC) Amazon. Le SCP suivant illustre ce processus.

Example politique refusant l'accès à Amazon S3 dans des conditions spécifiques

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:*"
```

```
            ],
            "Resource": "arn:aws:s3:::lambda_bucket/*",
            "Effect": "Deny",
            "Condition": {
                "StringNotEqualsIfExists": {
                    "aws:SourceVpc": [
                        "vpc-12345678"
                    ]
                }
            }
        },
        {
            "Action": [
                "s3:*"
            ],
            "Resource": "arn:aws:s3:::lambda_bucket/*",
            "Effect": "Deny",
            "Condition": {
                "ArnNotEqualsIfExists": {
                    "lambda:SourceFunctionArn": "arn:aws:lambda:us-
east-1:123456789012:function:source_lambda"
                }
            }
        }
    ]
}
```

Cette stratégie refuse toutes les actions S3 sauf si elles proviennent d'une fonction Lambda spécifique avec ARN `arn:aws:lambda:*:123456789012:function:source_lambda`, ou à moins qu'ils ne proviennent du VPC spécifié. L'opérateur `StringNotEqualsIfExists` indique à IAM de traiter cette condition uniquement si la clé `aws:SourceVpc` est présente dans la demande. De la même façon, IAM considère l'opérateur `ArnNotEqualsIfExists` uniquement si le `lambda:SourceFunctionArn` existe.

Octroi d'autres AWS accès des entités à vos fonctions événementielles

Pour autoriser d'autres Comptes AWS organisations et services à accéder à vos ressources Lambda, plusieurs options s'offrent à vous :

- Vous pouvez utiliser des politiques basées sur l'identité pour autoriser d'autres utilisateurs à accéder à vos ressources Lambda. Identity-based les politiques peuvent s'appliquer directement aux utilisateurs ou aux groupes et rôles associés à un utilisateur.
- Vous pouvez utiliser des politiques basées sur les ressources pour accorder à d'autres comptes et Services AWS autorisations l'accès à vos ressources Lambda. Lorsqu'un utilisateur essaie d'accéder à une ressource Lambda, Lambda prend en compte à la fois les stratégies basées sur l'identité appartenant à l'utilisateur et la stratégie basée sur une ressource appartenant aux ressources. Lorsqu'un AWS service tel qu'Amazon Simple Storage Service (Amazon S3) appelle votre fonction Lambda, Lambda ne prend en compte que la politique basée sur les ressources.
- Vous pouvez utiliser un modèle de contrôle d'accès par attributs (ABAC) pour contrôler l'accès à vos fonctions Lambda. Avec ABAC, vous pouvez attacher des balises à une fonction Lambda, les transmettre dans certaines requêtes d'API ou les attacher au principal IAM qui effectue la requête. Spécifiez les mêmes balises dans l'élément condition d'une politique IAM pour contrôler l'accès aux fonctions.

Pour vous aider à optimiser vos autorisations d'accès avec le moindre privilège, Lambda fournit des conditions supplémentaires que vous pouvez inclure dans vos politiques. Pour plus d'informations, consultez the section called "Ressources et conditions".

Identity-based Politiques IAM pour Lambda

Vous pouvez utiliser des politiques basées sur l'identité dans Gestion des identités et des accès AWS (IAM) pour autoriser les utilisateurs de votre compte à accéder à Lambda. Identity-based les politiques peuvent s'appliquer aux utilisateurs, aux groupes d'utilisateurs ou aux rôles. Vous pouvez également accorder aux utilisateurs d'un autre compte l'autorisation d'endosser un rôle de votre compte et d'accéder à vos ressources Lambda.

Lambda fournit des politiques AWS gérées qui accordent l'accès aux actions de l'API Lambda et, dans certains cas, à d'autres AWS services utilisés pour développer et gérer les ressources Lambda. Lambda met à jour ces stratégies gérées si nécessaire pour s'assurer que vos utilisateurs ont accès aux nouvelles fonctionnalités quand elles sont disponibles.

- AWS Lambda_FullAccess — Accorde un accès complet aux actions Lambda et aux autres AWS services utilisés pour développer et gérer les ressources Lambda.
- AWS Lambda_ReadOnlyAccess — Accorde un accès en lecture seule aux ressources Lambda.
- AWSLambdaRole— Accorde l'autorisation d'invoquer des fonctions d'événement.

AWS les politiques gérées autorisent les actions d'API sans restreindre les fonctions ou les couches Lambda qu'un utilisateur peut modifier. Pour bénéficier d'un contrôle plus précis, vous pouvez créer vos propres stratégies qui limitent la portée des autorisations d'un utilisateur. Pour plus d'informations sur l'octroi de l'accès aux couches, consultezthe section called “Accès à une couche”.

Rubriques

- Autoriser les utilisateurs à accéder à une fonction événementielle
- Octroi aux utilisateurs de l'accès à une couche Lambda

Autoriser les utilisateurs à accéder à une fonction événementielle

Utilisez des politiques basées sur l'identité pour autoriser les utilisateurs, les groupes d'utilisateurs ou les rôles à effectuer des opérations sur les fonctions d'événement Lambda.

> **Note**
>
> Pour une fonction définie comme une image de conteneur, l'autorisation des utilisateurs à accéder à l'image doit être configurée dans Amazon Elastic Container Registry (Amazon ECR). Pour voir un exemple, consultez la rubrique Politiques de référentiel Amazon ECR.

Voici un exemple de stratégie d'autorisations avec une portée limitée. Elle permet à un utilisateur de créer et gérer des fonctions Lambda nommées avec un préfixe distinct (`intern-`) et configurées avec un rôle d'exécution désigné.

Example Stratégie de développement des fonctions

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
```

```
        {
            "Sid": "ReadOnlyPermissions",
            "Effect": "Allow",
            "Action": [
                "lambda:GetAccountSettings",
                "lambda:GetEventSourceMapping",
                "lambda:GetFunction",
                "lambda:GetFunctionConfiguration",
                "lambda:GetFunctionCodeSigningConfig",
                "lambda:GetFunctionConcurrency",
                "lambda:ListEventSourceMappings",
                "lambda:ListFunctions",
                "lambda:ListTags",
                "iam:ListRoles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DevelopFunctions",
            "Effect": "Allow",
            "NotAction": [
                "lambda:AddPermission",
                "lambda:PutFunctionConcurrency"
            ],
            "Resource": "arn:aws:lambda:*:*:function:intern-*"
        },
        {
            "Sid": "DevelopEventSourceMappings",
            "Effect": "Allow",
            "Action": [
                "lambda:DeleteEventSourceMapping",
                "lambda:UpdateEventSourceMapping",
                "lambda:CreateEventSourceMapping"
            ],
            "Resource": "*",
            "Condition": {
                "ArnLike": {
                    "lambda:FunctionArn": "arn:aws:lambda:*:*:function:intern-*"
                }
            }
        },
        {
            "Sid": "PassExecutionRole",
            "Effect": "Allow",
```

```
            "Action": [
                "iam:ListRolePolicies",
                "iam:ListAttachedRolePolicies",
                "iam:GetRole",
                "iam:GetRolePolicy",
                "iam:PassRole",
                "iam:SimulatePrincipalPolicy"
            ],
            "Resource": "arn:aws:iam::*:role/intern-lambda-execution-role"
        },
        {
            "Sid": "ViewLogs",
            "Effect": "Allow",
            "Action": [
                "logs:*"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/lambda/intern-*"
        }
    ]
}
```

Les autorisations de la stratégie sont organisées en déclarations reposant sur les ressources et conditions qu'elles prennent en charge.

- `ReadOnlyPermissions` – La console Lambda utilise ces autorisations lorsque vous parcourez et affichez les fonctions. Les conditions ou modèles de ressources ne sont pas pris en charge.

```
        "Action": [
            "lambda:GetAccountSettings",
            "lambda:GetEventSourceMapping",
            "lambda:GetFunction",
            "lambda:GetFunctionConfiguration",
            "lambda:GetFunctionCodeSigningConfig",
            "lambda:GetFunctionConcurrency",
            "lambda:ListEventSourceMappings",
            "lambda:ListFunctions",
            "lambda:ListTags",
            "iam:ListRoles"
        ],
        "Resource": "*"
```

- `DevelopFunctions` – Utilisez toute action Lambda qui s'exécute sur des fonctions ayant le préfixe `intern-`, à l'exception de `AddPermission` et de `PutFunctionConcurrency`. `AddPermission` modifie la politique basée sur les ressources de la fonction, ce qui peut avoir des conséquences en matière de sécurité. `PutFunctionConcurrency` réserve la capacité de mise à l'échelle pour une fonction, et peut retirer de la capacité à d'autres fonctions.

```
        "NotAction": [
            "lambda:AddPermission",
            "lambda:PutFunctionConcurrency"
        ],
        "Resource": "arn:aws:lambda:*:*:function:intern-*"
```

- `DevelopEventSourceMappings` – Gérez les mappages de source d'événement sur les fonctions qui sont préfixées avec `intern-`. Ces actions s'exécutent sur des mappages de source d'événement, mais vous pouvez les restreindre par fonction à l'aide d'une condition.

```
        "Action": [
            "lambda:DeleteEventSourceMapping",
            "lambda:UpdateEventSourceMapping",
            "lambda:CreateEventSourceMapping"
        ],
        "Resource": "*",
        "Condition": {
            "StringLike": {
                "lambda:FunctionArn": "arn:aws:lambda:*:*:function:intern-*"
            }
        }
```

- `PassExecutionRole` – Affichez et transmettez uniquement un rôle nommé `intern-lambda-execution-role`, qui doit être créé et géré par un utilisateur avec des autorisations IAM. `PassRole` est utilisé lorsque vous attribuez un rôle d'exécution à une fonction.

```
        "Action": [
            "iam:ListRolePolicies",
            "iam:ListAttachedRolePolicies",
            "iam:GetRole",
            "iam:GetRolePolicy",
            "iam:PassRole",
```

```
            "iam:SimulatePrincipalPolicy"
        ],
        "Resource": "arn:aws:iam::*:role/intern-lambda-execution-role"
```

- `ViewLogs`— Utilisez CloudWatch les journaux pour afficher les journaux des fonctions préfixées par`intern-`.

```
        "Action": [
            "logs:*"
        ],
        "Resource": "arn:aws:logs:*:*:log-group:/aws/lambda/intern-*"
```

Cette stratégie permet à un utilisateur de démarrer avec Lambda, sans nuire aux ressources des autres utilisateurs. Il n'autorise pas un utilisateur à configurer une fonction à déclencher ou à appeler d'autres AWS services, ce qui nécessite des autorisations IAM plus étendues. Cela n'inclut pas non plus l'autorisation d'accéder aux services qui ne prennent pas en charge les politiques à portée limitée, tels que CloudWatch et. X-Ray Pour ces services, utilisez les stratégies en lecture seule afin d'accorder à l'utilisateur l'accès aux métriques et aux données de suivi.

Lorsque vous configurez des déclencheurs pour votre fonction, vous devez y accéder pour utiliser le AWS service qui appelle votre fonction. Par exemple, pour configurer un déclencheur Amazon S3, vous vous devez être autorisé à utiliser les actions Amazon S3 qui gèrent les notifications de compartiment. La plupart de ces autorisations sont incluses dans la politique Lambda_FullAccess gérée par AWS.

Octroi aux utilisateurs de l'accès à une couche Lambda

Utilisez des politiques basées sur l'identité pour autoriser des utilisateurs, des groupes d'utilisateurs ou des groupes à effectuer des opérations sur des couches Lambda. La stratégie suivante accorde à un utilisateur l'autorisation de créer des couches et de les utiliser avec des fonctions. Les modèles de ressources permettent à l'utilisateur de travailler dans n' Région AWS importe quelle version de couche, à condition que le nom de la couche commence par`test-`.

Example stratégie de développement des couches

JSON

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "PublishLayers",
            "Effect": "Allow",
            "Action": [
                "lambda:PublishLayerVersion"
            ],
            "Resource": "arn:aws:lambda:*:*:layer:test-*"
        },
        {
            "Sid": "ManageLayerVersions",
            "Effect": "Allow",
            "Action": [
                "lambda:GetLayerVersion",
                "lambda:DeleteLayerVersion"
            ],
            "Resource": "arn:aws:lambda:*:*:layer:test-*:*"
        }
    ]
}
```

Vous pouvez également appliquer l'utilisation des couches durant la création et la configuration de la fonction avec la condition `lambda:Layer`. Par exemple, vous pouvez empêcher les utilisateurs d'utiliser les couches publiées par d'autres comptes. La stratégie ci-dessous ajoute une condition aux actions `CreateFunction` et `UpdateFunctionConfiguration` afin d'exiger que toutes les couches spécifiées proviennent du compte `123456789012`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ConfigureFunctions",
            "Effect": "Allow",
            "Action": [
                "lambda:CreateFunction",
                "lambda:UpdateFunctionConfiguration"
            ],
            "Resource": "*",
```

```
            "Condition": {
                "ForAllValues:StringLike": {
                    "lambda:Layer": [
                        "arn:aws:lambda:*:123456789012:layer:*:*"
                    ]
                }
            }
        }
    ]
}
```

Pour que la condition s'applique, vérifiez qu'aucune autre déclaration n'accorde d'autorisation utilisateur à ces actions.

Utilisation de politiques basées sur les ressources dans Lambda

Grâce aux politiques d'autorisation basées sur les ressources, vous pouvez accorder à d'autres utilisateurs Comptes AWS, organisations et l' Services AWS accès à vos fonctions d'événement Lambda. Une politique basée sur les ressources est un document JSON qui contient une ou plusieurs instructions. Chaque déclaration définit les éléments suivants :

- `Principal`: L'entité à laquelle vous souhaitez accorder des autorisations (une autre Service AWS, un rôle ou un utilisateur IAM, ou autre Compte AWS)
- `Action`: liste des actions d'API que vous souhaitez autoriser ou refuser pour le principal spécifié
- `Effect`: si vous souhaitez autoriser ou refuser au principal la possibilité d'utiliser les actions d'API choisies
- `Resource`: la fonction, la version ou l'alias Lambda auxquels vous souhaitez appliquer l'instruction (vous pouvez également utiliser un caractère générique pour spécifier toutes les versions et alias de votre fonction)

Vous pouvez également utiliser des éléments facultatifs tels que `Sid` (un identifiant de déclaration) et `Condition` (des conditions logiques pour un contrôle d'accès précis). Pour obtenir la liste complète des éléments de stratégie pris en charge, reportez-vous à la référence des éléments de stratégie IAM JSON dans le guide de l'Gestion des identités et des accès AWS utilisateur.

Ajouter des autorisations basées sur les ressources à une fonction d'événement

Vous pouvez ajouter des autorisations basées sur les ressources à votre fonction Lambda à l'aide de deux méthodes :

- Politique JSON complète : utilisez la console Lambda ou l'action PutResourcePolicyAPI pour ajouter un document de politique JSON complet. AWS CLI Avec une politique JSON complète, vous pouvez utiliser la gamme complète des clés de condition globales IAM, ajouter plusieurs instructions avec plusieurs principes et créer des instructions explicitesDeny. La taille maximale d'une politique basée sur les ressources JSON est de 20 Ko.
- Autorisations individuelles : utilisez l'action de console ou d'AddPermissionAPI pour ajouter `Allow` des instructions uniques. Les autorisations individuelles ne prennent en charge qu'un ensemble limité de clés de condition (`aws:SourceArn`aws:SourceAccount, et`aws:PrincipalOrgID`).

Nous vous recommandons de définir des politiques JSON complètes pour ajouter des autorisations basées sur les ressources à votre fonction. La création d'une politique JSON complète vous donne plus de flexibilité et un contrôle précis de vos autorisations.

> **Important**
>
> L'utilisation `put-resource-policy` remplace toute politique basée sur les ressources existante sur la ressource. Si la ressource possède déjà des autorisations définies avec`add-permission`, les `put-resource-policy` remplace. `get-resource-policy`À utiliser pour récupérer la politique existante avant d'apporter des modifications.

Autorisations requises

Pour utiliser les actions`PutResourcePolicy`,`GetResourcePolicy`, et `DeleteResourcePolicy` API, vous devez disposer des autorisations IAM suivantes :

Action d’API	Autorisations requises
PutResourcePolicy	`lambda:PutResourcePolicy` , `lambda:AddPermission` et `lambda:RemovePermission`

Action d'API	Autorisations requises
GetResourcePolicy	`lambda:GetResourcePolicy` et `lambda:GetPolicy`
DeleteResourcePolicy	`lambda:DeleteResourcePolicy` et `lambda:RemovePermission`

Console

Pour créer une politique complète basée sur les ressources JSON

1. Ouvrez la page Event Functions de la console Lambda.
2. Sélectionnez la fonction à laquelle vous souhaitez autoriser l'accès, puis sélectionnez l'onglet Configuration.
3. Sélectionnez Autorisations.
4. Dans le volet des déclarations de Resource-based politique, choisissez Modifier. Cette action ouvre l'éditeur de politique JSON.
5. Ajoutez des instructions à la politique de votre fonction. Vous pouvez sélectionner des actions d'API, ajouter des principaux de différents types (services, comptes, rôles IAM) et ajouter des clés de condition pour contrôler l'accès.
6. Cliquez sur Enregistrer.

Vous pouvez également modifier la politique basée sur les ressources de votre fonction directement dans le volet Stratégie.

AWS CLI

Pour ajouter une politique complète basée sur les ressources JSON

Pour ajouter une politique JSON complète à votre fonction, utilisez la `put-resource-policy` AWS CLI commande.

L'exemple de commande suivant ajoute une politique basée sur les ressources à votre fonction à l'aide d'une politique définie dans un fichier nommé `policy.json` sur votre machine locale. Exécutez la commande depuis le répertoire qui contient le fichier. `resource-arn`Vous pouvez spécifier une version ou un alias de fonction, ou vous pouvez utiliser l'ARN de la fonction non qualifiée pour appliquer la politique à l'ensemble de la fonction.

```
aws lambda put-resource-policy --resource-arn arn:aws:lambda:us-
east-2:123456789012:function:my-function \
--policy file://policy.json
```

Lambda APIs

Pour ajouter une politique d'autorisation JSON complète à votre fonction, utilisez l'action PutResourcePolicyAPI. Vous pouvez également supprimer la politique d'une fonction à l'aide de l'DeleteResourcePolicyaction ou récupérer la politique actuellement attachée à une fonction à l'aide de l'GetResourcePolicyaction.

Pour ajouter des autorisations individuelles à la politique d'une fonction, utilisez l'action AddPermissionAPI.

Afficher la politique basée sur les ressources d'une fonction

Console

Pour afficher la stratégie basée sur les ressources d'une fonction

1. Ouvrez la page Event Functions de la console Lambda.
2. Choisissez une fonction.
3. Sélectionnez Configuration (Configuration), puis Permissions (Autorisations).
4. Faites défiler la page jusqu'aux déclarations de Resource-based politique pour voir la politique.

AWS CLI

Pour afficher une stratégie basée sur les ressources d'une fonction, utilisez la commande `get-resource-policy`. Vous pouvez utiliser l'ARN non qualifié de votre fonction ou spécifier une version ou un alias.

```
aws lambda get-resource-policy --resource-arn arn:aws:lambda:us-
east-2:123456789012:function:my-function
```

Vous pouvez également utiliser la `get-policy` commande :

```
aws lambda get-policy \
```

```
  --function-name my-function \
  --output text
```

Lambda APIs

Pour récupérer la politique basée sur les ressources d'une fonction, utilisez l'action GetResourcePolicyAPI. Vous pouvez utiliser l'ARN non qualifié de votre fonction ou spécifier une version ou un alias ARN.

Vous pouvez également utiliser l'action GetPolicyAPI.

Supprimer la politique basée sur les ressources d'une fonction

Console

Pour supprimer la politique basée sur les ressources d'une fonction

1. Ouvrez la page Event Functions de la console Lambda.
2. Sélectionnez la fonction pour laquelle vous souhaitez supprimer la politique d'autorisation.
3. Sélectionnez l'onglet Configuration, puis Autorisations.
4. Dans le volet des déclarations de Resource-based politique, choisissez Supprimer.

AWS CLI

Pour supprimer la politique de votre fonction, utilisez la `delete-resource-policy` commande et spécifiez l'ARN de la fonction, de la version ou de l'alias dont vous souhaitez supprimer la politique.

```
aws lambda delete-resource-policy --resource-arn arn:aws:lambda:us-
east-2:123456789012:function:my-function
```

Pour supprimer des déclarations individuelles, utilisez`remove-permission`.

```
aws lambda remove-permission \
  --function-name example \
  --statement-id sns
```

Lambda APIs

Pour supprimer la politique basée sur les ressources attachée à une fonction, à une version de fonction ou à un alias de fonction, utilisez l'action DeleteResourcePolicyAPI.

Pour supprimer des instructions individuelles d'une politique, utilisez l'action RemovePermissionAPI.

Mettre à jour les politiques existantes

Lorsque vous mettez à jour les autorisations basées sur les ressources existantes d'une fonction, le comportement dépend de la méthode que vous utilisez :

- `put-resource-policy`/PutResourcePolicy— Remplace l'intégralité de la politique existante. Toutes les autorisations individuelles précédemment ajoutées sont remplacées.
- `add-permission`/AddPermission— Ajoute une instruction à la politique existante sans la remplacer. Si vous appelez `add-permission` après`put-resource-policy`, la nouvelle instruction s'ajoute à la politique JSON existante.

Pour éviter de remplacer involontairement les autorisations existantes lors de l'utilisation`put-resource-policy`, récupérez d'abord la politique existante de votre fonction. La `get-resource-policy` sortie inclut un `RevisionId` champ.

```
aws lambda get-resource-policy --resource-arn arn:aws:lambda:us-east-2:123456789012:function:my-function
```

Lorsque vous attachez une nouvelle politique, indiquez la `RevisionId` valeur avec le `--revision-id` paramètre pour vous assurer que vous mettez à jour la dernière version. Si vous fournissez un ancien ID de révision, Lambda ne met pas à jour la politique de votre fonction.

```
aws lambda put-resource-policy \
  --resource-arn arn:aws:lambda:us-east-2:123456789012:function:my-function \
  --policy file://policy.json \
  --revision-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

> **Note**
>
> Les politiques basées sur les ressources existantes créées avec `AddPermission` continuent de fonctionner sans modification. Aucune modification de votre code de fonction n'est requise pour utiliser la nouvelle `PutResourcePolicy` API.

Bonnes pratiques de sécurité

Avec les politiques basées sur les ressources JSON, vous pouvez suivre des modèles d'accès avec le moindre privilège. Vous pouvez également satisfaire aux exigences réglementaires relatives aux refus explicites. Avec des politiques JSON complètes, vous pouvez :

- Créez des `Deny` déclarations explicites pour bloquer des principes ou des conditions spécifiques.
- Utilisez les conditions organisationnelles (`aws:PrincipalOrgID`,`aws:PrincipalOrgPaths`) pour restreindre l'accès à vos organisations sans énumérer les comptes individuels.
- Élargissez les autorisations à des comptes sources ou à des ARN spécifiques à l'aide de la gamme complète de clés de condition globales IAM.

Exemples de politiques basées sur les ressources

Example Octroi d'une autorisation à Amazon S3 avec une déclaration de refus

La politique suivante accorde à tous les compartiments Amazon S3 d'un compte l'autorisation d'invoquer une fonction, à l'exception d'un compartiment explicitement refusé.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "allow-s3",
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": "lambda:InvokeFunction",
            "Resource": "arn:aws:lambda:us-east-2:111122223333:function:my-function",
            "Condition": {
                "StringEquals": {
```

```
                    "aws:SourceAccount": "111122223333"
                }
            }
        },
        {
            "Sid": "deny-s3-bucket",
            "Effect": "Deny",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": "lambda:InvokeFunction",
            "Resource": [
                "arn:aws:lambda:us-east-2:111122223333:function:my-function",
                "arn:aws:lambda:us-east-2:111122223333:function:my-function:*"
            ],
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:s3:::amzn-s3-demo-bucket"
                }
            }
        }
    ]
}
```

Example Octroi d'autorisations aux comptes d'une organisation

La politique suivante accorde un accès invoqué à tous Comptes AWS les membres d'une organisation.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "org-access",
            "Effect": "Allow",
            "Action": "lambda:InvokeFunction",
            "Principal": "*",
            "Resource": "arn:aws:lambda:us-east-2:111122223333:function:my-function",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "o-a1b2c3d4e5f"
                }
            }
```

```
        }
    ]
}
```

Example Octroi d'autorisations à plusieurs rôles IAM sous certaines conditions

La politique suivante autorise deux rôles IAM à utiliser l' CreateAlias action à partir d'une adresse IP spécifiée.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "allow-roles",
            "Effect": "Allow",
            "Action": "lambda:CreateAlias",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::444455556666:role/role-name",
                    "arn:aws:iam::444455556666:role/role-name2"
                ]
            },
            "Resource": "arn:aws:lambda:us-east-2:111122223333:function:my-function",
            "Condition": {
                "IpAddress": {
                    "aws:SourceIp": "192.0.2.0"
                }
            }
        }
    ]
}
```

Example Refuser l'accès à moins que l'appelant ne fasse partie d'une organisation spécifiée

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "deny-access",
            "Effect": "Deny",
            "Action": "lambda:InvokeFunction",
            "Principal": "*",
```

```
            "Resource": "arn:aws:lambda:us-east-2:111122223333:function:my-function",
            "Condition": {
                "ForAllValues:StringNotLike": {
                    "aws:PrincipalOrgPaths": [
                        "o-a1b2c3d4e5/r-ab12/ou-ab12-11111111/*"
                    ]
                }
            }
        },
        {
            "Sid": "allow-access",
            "Effect": "Allow",
            "Action": "lambda:InvokeFunction",
            "Principal": "*",
            "Resource": "arn:aws:lambda:us-east-2:111122223333:function:my-function",
            "Condition": {
                "ForAnyValue:StringLike": {
                    "aws:PrincipalOrgPaths": [
                        "o-a1b2c3d4e5/r-ab12/ou-ab12-11111111/*"
                    ]
                }
            }
        }
    ]
}
```

Actions d'API prises en charge

Les actions de l'API Lambda suivantes prennent en charge les politiques basées sur les ressources :

- CreateAlias
- DeleteAlias
- DeleteFunction
- DeleteFunctionConcurrency
- DeleteFunctionEventInvokeConfig
- DeleteProvisionedConcurrencyConfig
- GetAlias
- GetFunction
- GetFunctionConcurrency

- GetFunctionConfiguration
- GetFunctionEventInvokeConfig
- GetPolicy
- GetProvisionedConcurrencyConfig
- Invoke
- InvokeFunctionUrl(autorisation uniquement)
- ListAliases
- ListFunctionEventInvokeConfigs
- ListProvisionedConcurrencyConfigs
- ListTags
- ListVersionsByFunction
- PublishVersion
- PutFunctionConcurrency
- PutFunctionEventInvokeConfig
- PutProvisionedConcurrencyConfig
- TagResource
- UntagResource
- UpdateAlias
- UpdateFunctionCode
- UpdateFunctionEventInvokeConfig

Accorder l'accès à la fonction événementielle Services AWS

Lorsque vous utilisez un AWS service pour appeler votre fonction, vous accordez l'autorisation dans une déclaration relative à une politique basée sur les ressources. Vous pouvez appliquer la déclaration à l'ensemble de la fonction, ou limiter la déclaration à une seule version ou un seul alias.

> **Note**
>
> Lorsque vous ajoutez un déclencheur à la fonction à l'aide de la console Lambda, celle-ci met à jour la stratégie basée sur une ressource de la fonction afin d'autoriser le service à

l'invoquer. Pour accorder des autorisations à d'autres comptes ou services non disponibles dans la console Lambda, vous pouvez utiliser l' AWS CLI.

Nous vous recommandons `put-resource-policy` de l'utiliser pour définir une politique JSON complète. Vous pouvez ainsi ajouter des déclarations de refus, utiliser la gamme complète des clés de condition IAM et gérer toutes les autorisations dans un seul document. `put-resource-policy` Vous pouvez également `add-permission` ajouter des instructions individuelles pour des cas d'utilisation simples.

Important

L'utilisation `put-resource-policy` remplace toute politique basée sur les ressources existante sur la ressource. Si la ressource possède déjà des autorisations définies avec`add-permission`, les `put-resource-policy` remplace. `get-resource-policy`À utiliser pour récupérer la politique existante avant d'apporter des modifications.

Utiliser une politique JSON complète (recommandé)

L'exemple de politique suivant accorde à Amazon Simple Notification Service l'autorisation d'appeler une fonction nommée`my-function`, mais uniquement pour un sujet spécifique. Il refuse également les invocations liées à un sujet particulier.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "allow-sns-my-topic",
            "Effect": "Allow",
            "Principal": {
                "Service": "sns.amazonaws.com"
            },
            "Action": "lambda:InvokeFunction",
            "Resource": "arn:aws:lambda:us-east-2:123456789012:function:my-function",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:sns:us-east-2:123456789012:my-topic"
                }
            }
```

```
        },
        {
            "Sid": "deny-sns-other-topic",
            "Effect": "Deny",
            "Principal": {
                "Service": "sns.amazonaws.com"
            },
            "Action": "lambda:InvokeFunction",
            "Resource": [
                "arn:aws:lambda:us-east-2:123456789012:function:my-function",
                "arn:aws:lambda:us-east-2:123456789012:function:my-function:*"
            ],
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:sns:us-east-2:123456789012:restricted-
topic"
                }
            }
        }
    ]
}
```

Enregistrez la politique dans un fichier nommé `policy.json` et appliquez-la avec `put-resource-policy` :

```
aws lambda put-resource-policy \
  --resource-arn arn:aws:lambda:us-east-2:123456789012:function:my-function \
  --policy file://policy.json
```

Pour Amazon S3, la source est un compartiment dont l'ARN n'inclut pas d'ID de compte. Il est possible que vous supprimiez un bucket et qu'un autre compte crée un bucket portant le même nom. Utilisez la clé de `aws:SourceAccount` condition pour vous assurer que seules les ressources de votre compte peuvent invoquer la fonction :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "allow-s3",
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
```

```
            },
            "Action": "lambda:InvokeFunction",
            "Resource": "arn:aws:lambda:us-east-2:123456789012:function:my-function",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:s3:::my-bucket"
                }
            }
        }
    ]
}
```

Utilisation de l'autorisation d'ajout

Pour les cas d'utilisation simples, vous pouvez `add-permission` ajouter des instructions individuelles. La commande suivante autorise Amazon Simple Notification Service à appeler une fonction nommée `my-function` :

```
aws lambda add-permission \
  --function-name my-function \
  --action lambda:InvokeFunction \
  --statement-id sns \
  --principal sns.amazonaws.com \
  --output text
```

Vous devriez voir la sortie suivante :

```
{"Sid":"sns","Effect":"Allow","Principal":
{"Service":"sns.amazonaws.com"},"Action":"lambda:InvokeFunction","Resource":"arn:aws:lambda:us-
east-2:123456789012:function:my-function"}
```

> **Note**
>
> Si vous appelez `add-permission` après`put-resource-policy`, la nouvelle instruction s'ajoute à la politique JSON existante.

Pour limiter les invocations à une ressource spécifique, utilisez l'`source-arn`option suivante :

```
aws lambda add-permission \
  --function-name my-function \
  --action lambda:InvokeFunction \
  --statement-id sns-my-topic \
  --principal sns.amazonaws.com \
  --source-arn arn:aws:sns:us-east-2:123456789012:my-topic
```

Pour Amazon S3, utilisez l'`source-account`option avec votre identifiant de compte :

```
aws lambda add-permission \
  --function-name my-function \
  --action lambda:InvokeFunction \
  --statement-id s3-account \
  --principal s3.amazonaws.com \
  --source-arn arn:aws:s3:::amzn-s3-demo-bucket \
  --source-account 123456789012
```

Octroi de l'accès à la fonction à une organisation

Pour accorder des autorisations à tous les comptes d'une AWS Organizationsorganisation, nous vous recommandons `put-resource-policy` de créer une politique JSON complète avec la clé de `aws:PrincipalOrgID` condition.

> **Important**
>
> L'utilisation `put-resource-policy` remplace toute politique basée sur les ressources existante sur la ressource. Si la ressource possède déjà des autorisations définies avec`add-permission`, les `put-resource-policy` remplace. `get-resource-policy`À utiliser pour récupérer la politique existante avant d'apporter des modifications.

Utiliser une politique JSON complète (recommandé)

L'exemple de politique suivant accorde l'accès invoqué à tous les membres Comptes AWS de l'organisation `o-a1b2c3d4e5f` :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "org-access",
```

```
            "Effect": "Allow",
            "Principal": "*",
            "Action": "lambda:InvokeFunction",
            "Resource": "arn:aws:lambda:us-east-2:123456789012:function:my-function",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "o-a1b2c3d4e5f"
                }
            }
        }
    ]
}
```

Enregistrez la politique dans un fichier nommé `policy.json` et appliquez-la :

```
aws lambda put-resource-policy \
  --resource-arn arn:aws:lambda:us-east-2:123456789012:function:my-function \
  --policy file://policy.json
```

Avec une politique JSON complète, vous pouvez également refuser l'accès à des comptes spécifiques au sein d'une organisation :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "allow-org",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "lambda:InvokeFunction",
            "Resource": "arn:aws:lambda:us-east-2:123456789012:function:my-function",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "o-a1b2c3d4e5f"
                }
            }
        },
        {
            "Sid": "deny-specific-account",
            "Effect": "Deny",
            "Principal": {
                "AWS": "arn:aws:iam::999888777666:root"
            },
```

```
            "Action": "lambda:InvokeFunction",
            "Resource": [
                "arn:aws:lambda:us-east-2:123456789012:function:my-function",
                "arn:aws:lambda:us-east-2:123456789012:function:my-function:*"
            ]
        }
    ]
}
```

Utilisation de l'autorisation d'ajout

Pour les cas d'utilisation simples, vous pouvez utiliser `add-permission` l'`principal-org-id`option. La commande suivante accorde l'accès à l'invocation à tous les utilisateurs de l'organisation `o-a1b2c3d4e5f` :

```
aws lambda add-permission \
  --function-name my-function \
  --statement-id org-access \
  --action lambda:InvokeFunction \
  --principal * \
  --principal-org-id o-a1b2c3d4e5f
```

> **Note**
>
> Dans cette commande, `Principal` est `*`. Cela signifie que tous les utilisateurs de l'organisation `o-a1b2c3d4e5f` obtiennent des autorisations d'invocation de fonction. Si vous spécifiez un rôle Compte AWS ou comme étant le`Principal`, seul ce principal obtient les autorisations d'invocation des fonctions, mais uniquement s'il fait également partie de l'`o-a1b2c3d4e5f`organisation.

Pour plus d'informations, consultez aws : PrincipalOrg ID dans le guide de l'utilisateur IAM.

Accorder l'accès à la fonction événementielle à d'autres comptes

Pour partager une fonction avec une autre Compte AWS, ajoutez une déclaration d'autorisations entre comptes à la politique basée sur les ressources de la fonction. Nous vous recommandons `put-resource-policy` de l'utiliser pour créer une politique JSON complète. Avec`put-resource-policy`, vous pouvez spécifier plusieurs principes, ajouter des conditions et créer des déclarations de refus. Vous pouvez également l'utiliser `add-permission` pour des cas d'utilisation simples.

> **Important**
>
> L'utilisation `put-resource-policy` remplace toute politique basée sur les ressources existante sur la ressource. Si la ressource possède déjà des autorisations définies avec`add-permission`, les `put-resource-policy` remplace. `get-resource-policy`À utiliser pour récupérer la politique existante avant d'apporter des modifications.

Utiliser une politique JSON complète (recommandé)

L'exemple de politique suivant accorde deux Comptes AWS autorisations pour appeler une fonction, l'une étant limitée à un rôle IAM spécifique :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "allow-account-invoke",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:root",
                    "arn:aws:iam::444455556666:role/cross-account-role"
                ]
            },
            "Action": "lambda:InvokeFunction",
            "Resource": "arn:aws:lambda:us-east-2:123456789012:function:my-function"
        }
    ]
}
```

Enregistrez la politique dans un fichier nommé `policy.json` et appliquez-la. Ils `resource-arn` peuvent spécifier une fonction, une version ou un alias :

```
aws lambda put-resource-policy \
  --resource-arn arn:aws:lambda:us-east-2:123456789012:function:my-function \
  --policy file://policy.json
```

Vous pouvez également restreindre l'accès entre comptes à des versions spécifiques à l'aide d'un alias. La politique suivante autorise l'accès par appel uniquement via l'`prod`alias :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "allow-account-prod-alias",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": "lambda:InvokeFunction",
            "Resource": "arn:aws:lambda:us-east-2:123456789012:function:my-
function:prod"
        }
    ]
}
```

Enregistrez cette politique dans un fichier nommé `alias-policy.json` et appliquez-la à l'alias :

```
aws lambda put-resource-policy \
  --resource-arn arn:aws:lambda:us-east-2:123456789012:function:my-function:prod \
  --policy file://alias-policy.json
```

La stratégie basée sur les ressources accorde à l'autre compte l'autorisation d'accéder à la fonction, mais n'autorise pas les utilisateurs de ce compte à dépasser leurs autorisations. Les utilisateurs de l'autre compte doivent disposer des autorisations utilisateur correspondantes pour utiliser l'API Lambda.

Vous pouvez accorder l'accès entre comptes pour n'importe quelle action d'API qui s'exécute sur une fonction existante. Par exemple, vous pouvez accorder l'accès à `lambda:ListAliases` afin qu'un compte puisse obtenir une liste des alias ou à `lambda:GetFunction` pour qu'il puisse télécharger le code de votre fonction.

Pour accorder à d'autres comptes l'autorisation pour plusieurs fonctions ou pour des actions qui ne s'exécutent pas sur une fonction, nous vous conseillons d'utiliser des rôles IAM.

Utilisation de l'autorisation d'ajout

Pour les cas d'utilisation simples, vous pouvez `add-permission` ajouter des instructions individuelles. L'exemple suivant autorise le compte `111122223333` à invoquer `my-function` avec l'`prod`alias :

```
aws lambda add-permission \
  --function-name my-function:prod \
  --statement-id xaccount \
  --action lambda:InvokeFunction \
  --principal 111122223333 \
  --output text
```

Vous devriez voir la sortie suivante :

```
{"Sid":"xaccount","Effect":"Allow","Principal":
{"AWS":"arn:aws:iam::111122223333:root"},"Action":"lambda:InvokeFunction","Resource":"arn:aws:l
east-1:123456789012:function:my-function"}
```

> **Note**
>
> Si vous appelez `add-permission` après`put-resource-policy`, la nouvelle instruction s'ajoute à la politique JSON existante.

Afin de limiter l'accès à un utilisateur ou à un rôle dans un autre compte, spécifiez l'ARN complet de l'identité en tant que principal. Par exemple : `arn:aws:iam::123456789012:user/developer`.

Octroi de l'accès de la couche Lambda à d'autres comptes

Pour partager une couche avec une autre Compte AWS, ajoutez une déclaration d'autorisations entre comptes à la politique basée sur les ressources de la couche. Exécutez la add-layer-version-permissioncommande et spécifiez l'ID du compte sous la forme`principal`. Dans chaque instruction, vous pouvez accorder une autorisation à un compte unique, à tous les comptes ou à une organisation dans AWS Organizations.

L'exemple suivant autorise le compte 111122223333 à accéder à la version 2 de la couche `bash-runtime`.

```
aws lambda add-layer-version-permission \
  --layer-name bash-runtime \
  --version-number 2 \
  --statement-id xaccount \
  --action lambda:GetLayerVersion \
  --principal 111122223333 \
  --output text
```

Vous devez voir des résultats similaires à ce qui suit :

```
{"Sid":"xaccount","Effect":"Allow","Principal":
{"AWS":"arn:aws:iam::111122223333:root"},"Action":"lambda:GetLayerVersion","Resource":"arn:aws:
east-1:123456789012:layer:bash-runtime:2"}
```

Les autorisations ne s'appliquent qu'à une seule version de couche. Répétez le processus chaque fois que vous créez une nouvelle version de la couche.

Pour accorder l'autorisation à tous les comptes d'une organisation AWS Organizations, utilisez l'option `organization-id`. L'exemple suivant accorde à tous les comptes d'une organisation `o-t194hfs8cz` l'autorisation d'utiliser la version 3 de `my-layer`.

```
aws lambda add-layer-version-permission \
  --layer-name my-layer \
  --version-number 3 \
  --statement-id engineering-org \
  --principal '*' \
  --action lambda:GetLayerVersion \
  --organization-id o-t194hfs8cz \
  --output text
```

Vous devriez voir la sortie suivante :

```
{"Sid":"engineering-
org","Effect":"Allow","Principal":"*","Action":"lambda:GetLayerVersion","Resource":"arn:aws:lam
east-2:123456789012:layer:my-layer:3","Condition":{"StringEquals":
{"aws:PrincipalOrgID":"o-t194hfs8cz"}}}"
```

Pour octroyer l'autorisation à plusieurs comptes ou organisations, vous devez ajouter plusieurs instructions.

Utilisation du contrôle d'accès basé sur les attributs dans Lambda

Avec le Contrôle d'accès par attributs (ABAC), vous pouvez utiliser des balises pour contrôler l'accès à vos fonctions Lambda. Vous pouvez associer des balises à certaines ressources Lambda, à certaines demandes d'API ou au principal Gestion des identités et des accès AWS (IAM) émetteur de la demande. Pour plus d'informations sur la manière dont l'accès basé sur les attributs est AWS accordé, consultez la section Contrôle de l'accès aux AWS ressources à l'aide de balises dans le guide de l'utilisateur IAM.

Vous pouvez utiliser ABAC pourAccorder le moindre privilège sans spécifier ni un nom ni un modèle ARN Amazon Resource Name (ARN) dans la stratégie IAM. Au lieu de cela, vous pouvez spécifier une balise dans le champ élément de condition d'une stratégie IAM pour le contrôle de l'accès. La mise à l'échelle est plus facile avec ABAC, car vous n'avez pas à mettre à jour vos politiques IAM lorsque vous créez de nouvelles ressources. Ajoutez plutôt des balises aux nouvelles ressources pour contrôler l'accès.

Dans Lambda, les balises sont utilisées sur les ressources suivantes :

- Fonctions : pour plus d'informations sur les fonctions de balisage, voir the section called "Étiquettes".
- Configurations de signature de code : pour plus d'informations sur le balisage des configurations de signature de code, voir the section called "Balises de configuration de signature de code".
- Mappage des sources d'événements : pour plus d'informations sur le balisage du mappage des sources d'événements, voir the section called "Balises de mappage des sources d'événements".

Les balises ne sont pas prises en charge pour les couches.

Vous pouvez utiliser les clés de condition suivantes pour écrire des règles de politique IAM basées sur les balises :

- aws : ResourceTag/tag-key : Contrôlez l'accès en fonction des balises associées à une ressource Lambda.
- aws : RequestTag/tag-key : Exiger la présence de balises dans une demande, par exemple lors de la création d'une nouvelle fonction.
- aws : PrincipalTag/tag-key : Contrôlez ce que le principal IAM (la personne qui fait la demande) est autorisé à faire en fonction des balises associées à son utilisateur ou à son rôle IAM.
- aws : TagKeys : Contrôle si des clés de balise spécifiques peuvent être utilisées dans une requête.

Vous ne pouvez définir des conditions que pour les actions qui les prennent en charge. Pour obtenir une liste des conditions prises en charge par chaque action Lambda, consultez la rubrique Actions, ressources et clés de condition pour AWS Lambda dans la Référence de l'autorisation de service. Pour aws : ResourceTag/tag-key support, reportez-vous à « Types de ressources définis par » AWS Lambda. Pour le TagKeys support d'aws : RequestTag/tag-key et aws :, reportez-vous à « Actions définies par » AWS Lambda.

Rubriques

- Sécurisation de vos fonctions par balise

Sécurisation de vos fonctions par balise

Les étapes suivantes illustrent une façon de configurer des autorisations pour les fonctions à l'aide d'ABAC. Dans cet exemple de scénario, vous allez créer quatre stratégies d'autorisations IAM. Vous allez ensuite associer ces stratégies à un nouveau rôle IAM. Enfin, vous allez créer un utilisateur IAM et lui donner l'autorisation d'assumer le nouveau rôle.

Rubriques

- Conditions préalables
- Étape 1 : Exiger des balises pour les nouvelles fonctions
- Étape 2 : Autoriser les actions basées sur les balises associées à une fonction d'événement et à un principal IAM
- Étape 3 : Accorder des permissions de liste
- Étape 4 : accorder des autorisations IAM
- Étape 5 : Création du rôle IAM
- Étape 6 : Création d'un utilisateur IAM
- Étape 7 : Tester les autorisations
- Étape 8 : Nettoyer vos ressources

Conditions préalables

Assurez-vous que vous disposez d'un rôle d'exécution Lambda. Vous utiliserez ce rôle lorsque vous accorderez des autorisations IAM et lorsque vous créerez une fonction d'événement.

Étape 1 : Exiger des balises pour les nouvelles fonctions

Lorsque vous utilisez ABAC avec Lambda, il est recommandé d'exiger que toutes les fonctions comportent des balises. Cela permet de garantir que vos politiques d'autorisation ABAC fonctionnent comme prévu.

Créez une stratégie IAM similaire à l'exemple suivant : Cette politique utilise les clés de TagKeys condition aws : ResourceTag/tag-key, aws : et aws : pour exiger que les nouvelles fonctions et le principal IAM qui les crée possèdent tous deux la `project` balise. RequestTag/tag-key Le `ForAllValues` modificateur garantit que `project` est la seule balise autorisée. Si vous n'incluez

pas`ForAllValues`, les utilisateurs peuvent ajouter d'autres balises à la fonction tant qu'ils transmettent également `project`.

Example— Exiger des balises sur les nouvelles fonctions

JSON

```
{
    "Version":"2012-10-17",
    "Statement": {
      "Effect": "Allow",
      "Action": [
        "lambda:CreateFunction",
        "lambda:TagResource"
      ],
      "Resource": "arn:aws:lambda:*:*:function:*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/project": "${aws:PrincipalTag/project}",
          "aws:ResourceTag/project": "${aws:PrincipalTag/project}"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": "project"
        }
      }
    }
  }
```

Étape 2 : Autoriser les actions basées sur les balises associées à une fonction d'événement et à un principal IAM

Créez une deuxième politique IAM à l'aide de la clé de ResourceTag/tag-key condition aws : pour exiger que la balise du principal corresponde à la balise attachée à la fonction. L'exemple de stratégie suivant autorise les mandataires avec la balise `project` pour appeler des fonctions avec la balise `project`. Si une fonction possède d'autres balises, l'action est refusée.

Example— Exiger des balises correspondantes sur la fonction et le principal IAM

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
          "lambda:InvokeFunction",
          "lambda:GetFunction"
        ],
        "Resource": "arn:aws:lambda:*:*:function:*",
        "Condition": {
          "StringEquals": {
            "aws:ResourceTag/project": "${aws:PrincipalTag/project}"
          }
        }
      }
    ]
  }
```

Étape 3 : Accorder des permissions de liste

Créez une stratégie qui permet au principal de répertorier les fonctions Lambda et les rôles IAM. Cela permet au principal de voir toutes les fonctions Lambda et les rôles IAM sur la console et lors de l'appel des actions d'API.

Example— Accordez des autorisations de liste Lambda et IAM

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
      {
        "Sid": "AllResourcesLambdaNoTags",
        "Effect": "Allow",
        "Action": [
```

```
            "lambda:GetAccountSettings",
            "lambda:ListFunctions",
            "iam:ListRoles"
          ],
          "Resource": "*"
        }
      ]
    }
```

Étape 4 : accorder des autorisations IAM

Créez une politique qui autorise iam : PassRole. Cette autorisation est requise lorsque vous attribuez un rôle d'exécution à une fonction. Dans l'exemple de stratégie suivant, remplacez l'exemple d'ARN par l'ARN de votre rôle d'exécution Lambda.

> **Note**
>
> N'utilisez pas la clé de condition `ResourceTag` dans une politique avec l'action `iam:PassRole`. Vous ne pouvez pas utiliser la balise sur un rôle IAM pour contrôler l'accès aux personnes qui peuvent transmettre ce rôle. Pour plus d'informations sur les autorisations requises pour transmettre un rôle à un service, consultez la section Octroi à un utilisateur des autorisations pour transmettre un rôle à un AWS service.

Example— Accordez l'autorisation de transmettre le rôle d'exécution

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
      {
        "Sid": "VisualEditor0",
        "Effect": "Allow",
        "Action": [
          "iam:PassRole"
        ],
        "Resource": "arn:aws:iam::111122223333:role/lambda-ex"
      }
    ]
```

```
}
```

Étape 5 : Création du rôle IAM

C'est une bonne pratique d'utilisation des rôles pour déléguer des autorisations. Créer un rôle IAM appelé `abac-project-role` :

- Sur Étape 1 : Sélection d'une entité de confiance : Choisissez :AWS compte, puis Ce compte.
- Sur Étape 2 : Ajouter des autorisations : Joignez les quatre stratégies IAM que vous avez créées au cours des étapes précédentes.
- Sur Étape 3 : Nommer, vérifier et créer : Choisissez :Ajouter une balise. Pour Key (Clé), saisissez `project`. Ne saisissez pas Valeur.

Étape 6 : Création d'un utilisateur IAM

Création d'un utilisateur IAM appelé`abac-test-user`. Sur la page Définir des autorisations, choisissez Attacher directement les stratégies existantes, puis choisissez Créer une stratégie. Entrez la définition de politique suivante. Remplacez *111122223333* par votre ID de compte AWS. Cette stratégie permet à `abac-test-user` d'assumer `abac-project-role`.

Example— Autoriser l'utilisateur IAM à assumer le rôle ABAC

JSON

```
{
    "Version":"2012-10-17",
    "Statement": {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::111122223333:role/abac-project-role"
    }
  }
```

Étape 7 : Tester les autorisations

1. Connectez-vous à la AWS console en tant que`abac-test-user`. Pour plus d'informations, connectez-vous en tant qu'utilisateur IAM.

2. Basculez vers le rôle `abac-project-role`. Pour plus d'informations, consultez Changement de rôles (console).
3. Création d'une fonction Lambda.
   - Sous Autorisations Choisissez Modifier le rôle d'exécution par défaut, puis dans le champ Rôle d'exécution, choisissez Utiliser un rôle existant. Choisissez le même rôle d'exécution que celui que vous avez utilisé dansÉtape 4 : accorder des autorisations IAM.
   - Sous Paramètres avancés, choisissez Activer les balises, puis Ajouter un nouveau tag. Pour Key (Clé), saisissez `project`. Ne saisissez pas Valeur.
4. Test de la fonction.
5. Créez une deuxième fonction Lambda et ajoutez une balise différente, telle que`environment`. Cette opération devrait échouer car la stratégie ABAC que vous avez créée dans Étape 1 : Exiger des balises pour les nouvelles fonctions autorise uniquement le principal à créer des fonctions avec la balise `project`.
6. Créez une troisième fonction sans balises. Cette opération devrait échouer car la stratégie ABAC que vous avez créée dansÉtape 1 : Exiger des balises pour les nouvelles fonctionsne permet pas au mandant de créer des fonctions sans balises.

Grâce à cette stratégie d'autorisation, vous pouvez contrôler l'accès sans créer de nouvelles politiques pour chaque nouvel utilisateur. Pour accorder l'accès à de nouveaux utilisateurs, il suffit de leur donner l'autorisation d'assumer le rôle qui correspond au projet qui leur a été attribué.

Étape 8 : Nettoyer vos ressources

Suppression du rôle IAM

1. Ouvrez la page Roles (Rôles) de la console IAM.
2. Sélectionnez le rôle que vous avez créé à l'étape 5.
3. Sélectionnez Supprimer.
4. Pour confirmer la suppression, saisissez le nom du rôle dans la zone de saisie de texte.
5. Sélectionnez Supprimer.

Pour supprimer l'utilisateur IAM

1. Ouvrez la page Utilisateurs de la console IAM.

2. Sélectionnez l'utilisateur IAM que vous avez créé à l'étape 6.
3. Sélectionnez Supprimer.
4. Pour confirmer la suppression, saisissez le nom de l'utilisateur dans la zone de saisie de texte.
5. Choisissez Delete user (Supprimer l'utilisateur).

Pour supprimer la fonction d'événement Lambda

1. Ouvrez la page Event Functions de la console Lambda.
2. Sélectionnez la fonction d'événement que vous avez créée.
3. Sélectionnez Actions, Supprimer.
4. Saisissez **`confirm`** dans la zone de saisie de texte et choisissez Delete (Supprimer).

Fine-tuning les sections Ressources et Conditions des politiques

Vous pouvez restreindre la portée des autorisations d'un utilisateur en spécifiant des ressources et des conditions dans une stratégie IAM Gestion des identités et des accès AWS . Chaque action d'une politique prend en charge une combinaison de types de ressources et de conditions qui varie en fonction du comportement de l'action.

Chaque déclaration de stratégie IAM accorde une autorisation pour une action effectuée sur une ressource. Lorsque l'action n'agit pas sur une ressource nommée, ou lorsque vous accordez l'autorisation d'effectuer l'action sur toutes les ressources, la valeur de la ressource de la stratégie est un caractère générique (*). Pour la plupart des actions, vous pouvez limiter les ressources qu'un utilisateur peut modifier en spécifiant l'Amazon Resource Name (ARN) d'une ressource ou un modèle ARN qui correspond à plusieurs ressources.

Par type de ressource, la conception générale pour restreindre la portée d'une action est la suivante :

- Fonctions : les actions sur une fonction peuvent être limitées à une fonction spécifique selon l'ARN de la fonction, de la version ou de l'alias.
- Mappage des sources d'événements : les actions peuvent être limitées à des ressources de mappage des sources d'événements spécifiques selon l'ARN. Le mappage des sources d'événements est toujours associé à une fonction. Vous pouvez également utiliser la condition `lambda:FunctionArn` pour restreindre les actions par fonction associée.
- Couches : les actions liées à l'utilisation et aux autorisations relatives aux couches agissent sur les versions de couche.

- Configuration de signature de code : les actions peuvent être limitées à des ressources de configuration de signature de code spécifiques selon l'ARN.
- Balises : utilisez les conditions de balise standard. Pour plus d'informations, consultez the section called "Attribute-based contrôle d'accès".

Pour limiter les autorisations par ressource, spécifiez la ressource par son ARN.

Format ARN de ressource Lambda

- Fonction – `arn:aws:lambda:us-west-2:123456789012:function:my-function`
- Version de la fonction – `arn:aws:lambda:us-west-2:123456789012:function:my-function:1`
- Alias de la fonction – `arn:aws:lambda:us-west-2:123456789012:function:my-function:TEST`
- Exécution durable — `arn:aws:lambda:us-west-2:123456789012:function:my-function:1/durable-execution/execution-name/execution-id`
- Mappage de source d'événement – `arn:aws:lambda:us-west-2:123456789012:event-source-mapping:fa123456-14a1-4fd2-9fec-83de64ad683de6d47`
- Couche – `arn:aws:lambda:us-west-2:123456789012:layer:my-layer`
- Version de la couche – `arn:aws:lambda:us-west-2:123456789012:layer:my-layer:1`
- Configuration de signature de code – `arn:aws:lambda:us-west-2:123456789012:code-signing-config:my-csc`

Par exemple, la politique suivante permet Compte AWS `123456789012` à un utilisateur d'appeler une fonction nommée `my-function` dans la AWS région USA Ouest (Oregon).

Example appeler une stratégie de fonction

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "Invoke",
            "Effect": "Allow",
```

```
            "Action": [
                "lambda:InvokeFunction"
            ],
            "Resource": "arn:aws:lambda:us-west-2:123456789012:function:my-
function"
        }
    ]
}
```

Il s'agit d'un cas particulier, où l'identificateur de l'action (`lambda:InvokeFunction`) diffère de l'opération d'API (Appeler). Pour les autres actions, l'identificateur de l'action est le nom de l'opération avec le préfixe `lambda:`.

Sections

- Comprendre la section Condition relative aux stratégies
- Fonctions de référencement dans la section Ressources relative aux stratégies
- Référencer les exécutions durables dans la section Ressources des politiques
- Actions IAM et comportements de fonctions pris en charge

Comprendre la section Condition relative aux stratégies

Les conditions sont facultatives dans la stratégie, et appliquent une logique supplémentaire pour déterminer si une action est autorisée. Outre les conditions courantes prises en charge par toutes les actions, Lambda définit les types de condition que vous pouvez utiliser pour restreindre les valeurs des paramètres supplémentaires sur certaines actions.

Par exemple, la condition `lambda:Principal` permet de restreindre le service ou le compte auquel un utilisateur peut accorder l'accès d'invocation selon la stratégie basée sur les ressources d'une fonction. La stratégie suivante permet à un utilisateur d'accorder une autorisation à des rubriques Amazon Simple Notification Service (Amazon SNS) d'appeler une fonction nommée `test`.

Example gestion des autorisations d'une stratégie de fonction

JSON

```
{
    "Version":"2012-10-17",
```

```
    "Statement": [
        {
            "Sid": "ManageFunctionPolicy",
            "Effect": "Allow",
            "Action": [
                "lambda:AddPermission",
                "lambda:RemovePermission"
            ],
            "Resource": "arn:aws:lambda:us-west-2:123456789012:function:test:*",
            "Condition": {
                "StringEquals": {
                    "lambda:Principal": "sns.amazonaws.com"
                }
            }
        }
    ]
}
```

La condition nécessite que le principal soit Amazon SNS et pas un autre service ou compte. Le modèle de ressource exige que le nom de la fonction soit `test` et inclue un numéro de version ou un alias. Par exemple : `test:v1`.

Pour plus d'informations sur les ressources et les conditions de Lambda et d'autres AWS services, consultez la section Actions, ressources et clés de condition pour les AWS services dans la référence d'autorisation de service.

Fonctions de référencement dans la section Ressources relative aux stratégies

Vous référencez une fonction d'événement Lambda dans une déclaration de politique à l'aide d'un Amazon Resource Name (ARN). Le format de l'ARN d'une fonction dépend du fait que vous référenciez la fonction entière, la version d'une fonction ou un alias.

Lors des appels d'API Lambda, les utilisateurs peuvent spécifier une version ou un alias en transmettant un ARN de version ou un ARN d'alias dans le GetFunction`FunctionName`paramètre, ou en définissant une valeur dans le GetFunction`Qualifier`paramètre. Lambda prend des décisions d'autorisation en comparant l'élément de ressource dans la stratégie IAM au `FunctionName` et au `Qualifier` transmis dans les appels d'API. En cas d'incompatibilité, Lambda refuse la demande.

Que vous autorisiez ou refusiez une action sur votre fonction, vous devez utiliser les types ARN de fonction appropriés dans votre déclaration de stratégie pour obtenir les résultats attendus. Par

exemple, si votre stratégie fait référence à l'ARN non qualifié, Lambda accepte les demandes faisant référence à l'ARN non qualifié, mais refuse les demandes faisant référence à un ARN qualifié.

> **Note**
>
> Vous ne pouvez pas utiliser un caractère générique (*) pour établir une correspondance avec l'ID du compte. Pour plus d'informations sur la syntaxe acceptée, consultezRéférence de politique JSON IAMdans leIAM User Guide.

Example permettant l'invocation d'un ARN non qualifié

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "lambda:InvokeFunction",
            "Resource": "arn:aws:lambda:us-
west-2:123456789012:function:myFunction"
        }
    ]
}
```

Si votre stratégie fait référence à un ARN qualifié spécifique, Lambda accepte les demandes faisant référence à cet ARN, mais refuse les demandes faisant référence à l'ARN non qualifié ou à un ARN qualifié différent, par exemple,`myFunction:2`.

Example permettant l'invocation d'un ARN qualifié spécifique

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
```

```
            "Action": "lambda:InvokeFunction",
            "Resource": "arn:aws:lambda:us-
west-2:123456789012:function:myFunction:1"
        }
    ]
}
```

Si votre stratégie fait référence à un ARN qualifié à l'aide de `:*`, Lambda accepte tout ARN qualifié mais refuse les demandes faisant référence à l'ARN non qualifié.

Example permettant l'invocation de n'importe quel ARN qualifié

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "lambda:InvokeFunction",
            "Resource": "arn:aws:lambda:us-
west-2:123456789012:function:myFunction:*"
        }
    ]
}
```

Si votre stratégie fait référence à un ARN utilisant `*`, Lambda accepte tout ARN qualifié ou non qualifié.

Example permettant l'invocation de tout ARN qualifié ou non qualifié

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "lambda:InvokeFunction",
```

```
            "Resource": "arn:aws:lambda:us-
west-2:123456789012:function:myFunction*"
        }
    ]
}
```

Référencer les exécutions durables dans la section Ressources des politiques

Une exécution durable est une sous-ressource d'une version de fonction. Pour la structure ARN d'exécution durable et les directives en matière de politique, voirthe section called “Autorisations IAM pour des fonctions durables”.

Vous ne pouvez appeler des fonctions durables qu'avec un nom de fonction qualifié ou un ARN. Les politiques autorisant l'invocation de fonctions durables doivent donc correspondre aux ARN qualifiés. Pour plus d’informations, consultez the section called “Exigence d'ARN qualifiés”.

Si votre politique fait référence à l'ARN de la fonction non qualifiée, Lambda refuse les demandes d'actions d'exécution durables. L'ARN non qualifié ne correspond jamais à un ARN d'exécution durable.

Example Politique qui ne donne pas accès à des exécutions durables

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "lambda:GetDurableExecution",
            "Resource": "arn:aws:lambda:us-
west-2:123456789012:function:myDurableFunction"
        }
    ]
}
```

Si votre politique fait référence à la fonction ARN with`:*`, Lambda accepte les demandes d'exécution durable de chaque version.

Example Permettre l'accès à des exécutions durables de n'importe quelle version

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "lambda:GetDurableExecution",
            "Resource": "arn:aws:lambda:us-
west-2:123456789012:function:myDurableFunction:*"
        }
    ]
}
```

Si votre politique fait référence à la fonction ARN with`:1/durable-execution/*`, Lambda accepte les demandes d'exécutions durables de la version 1 uniquement.

Example Permettre l'accès à des exécutions durables d'une version spécifique

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "lambda:GetDurableExecution",
            "Resource": "arn:aws:lambda:us-
west-2:123456789012:function:myDurableFunction:1/durable-execution/*"
        }
    ]
}
```

⚠ Les modèles d'alias ne correspondent jamais aux ARN d'exécution durables

Les noms d'alias n'apparaissent jamais dans les ARN d'exécution durable. Un modèle de ressource tel que `my-function:prod/durable-execution/*` ne correspond jamais à une exécution durable car Lambda résout l'alias en un numéro de version lorsque la fonction s'exécute.

Lambda autorise l'`lambda:ListDurableExecutionsByFunction`action contre l'ARN de la fonction à partir de la demande, et non sur un ARN d'exécution durable. Les règles suivantes s'appliquent à la correspondance des ARN :

- Une politique qui accorde l'ARN à la fonction non qualifiée correspond uniquement aux demandes qui utilisent le nom de la fonction non qualifiée.

- Une politique qui accorde un ARN qualifié correspond uniquement aux demandes qui utilisent un nom de fonction qualifié.

Example Autoriser la liste des exécutions durables sous l'une ou l'autre forme de nom

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "lambda:ListDurableExecutionsByFunction",
            "Resource": [
                "arn:aws:lambda:us-west-2:123456789012:function:myDurableFunction",
                "arn:aws:lambda:us-west-2:123456789012:function:myDurableFunction:*"
            ]
        }
    ]
}
```

Actions IAM et comportements de fonctions pris en charge

Les actions définissent ce qui peut être autorisé par le biais des politiques IAM. Pour obtenir une liste des actions prises en charge par Lambda, consultez la rubrique Actions, ressources et clés de condition pour AWS Lambda dans la Référence de l'autorisation de service. Dans la plupart des cas, lorsqu'une action IAM autorise une action d'API Lambda, le nom de l'action IAM est identique à celui de l'action d'API Lambda, à l'exception des actions suivantes :

Action d'API	Action IAM
Invoke	`lambda:InvokeFunction`
GetLayerVersion GetLayerVersionByArn	`lambda:GetLayerVersion`

Outre les ressources et les conditions définies dans la référence d'autorisation de service, Lambda prend en charge les ressources et conditions suivantes pour certaines actions. Nombre d'entre elles sont liées aux fonctions de référencement dans la section des ressources relative aux politiques. Les

actions sur une fonction peuvent être limitées à une fonction spécifique selon l'ARN de la fonction, de la version ou de l'alias, tel que décrit dans le tableau suivant.

Action	Ressource	Condition
AddPermission RemovePermission Invoquer (Autorisation : `lambda:InvokeFunction`)	Version de la fonction Alias de la fonction	N/A
ListDurableExecutionsByFunction	Version de la fonction	N/A
UpdateFunctionConfiguration	N/A	`lambda:CodeSigningConfigArn`
CreateFunctionUrlConfig DeleteFunctionUrlConfig GetFunctionUrlConfig UpdateFunctionUrlConfig	Alias de la fonction	N/A

AWS Fonctions Web Lambda

Avec AWS Lambda Web Functions, vous pouvez exécuter des applications Web et des backends d'API en tant que serveurs HTTP sans serveur. Votre code écoute sur un port réseau et gère directement les demandes. Vous pouvez utiliser des frameworks Node.js Web familiers tels que ExpressHono, ou React Router sans Lambda-specific adaptateurs ou wrappers. Vous développez et exécutez votre serveur localement comme n'importe quelle autre application Node.js Web.

Vous déployez votre code sous forme de fichier .zip. Lambda crée un point de terminaison HTTPS, gère les environnements d'exécution et adapte votre application en fonction du trafic, y compris jusqu'à zéro lorsqu'elle est inactive. Pour réduire le temps de latence pour les utilisateurs répartis dans le monde entier, vous pouvez effectuer un déploiement sur plusieurs terminaux Régions AWS derrière un seul point de terminaison. Lambda utilise un routage basé sur la latence pour envoyer chaque demande à l'une de ces régions. Vous payez pour les demandes, le temps processeur actif, la mémoire consommée pendant la durée de vie de chaque environnement d'exécution et le transfert de données.

Rubriques

- Quand utiliser les fonctions Web
- Fonctionnement des fonctions Web
- Principaux avantages
- Concepts de base
- Création d'une fonction Web Lambda
- Déploiement de fonctions Web
- Requêtes et réponses HTTP
- Configuration de la mise en réseau pour AWS Lambda Fonctions Web
- Comportement de dimensionnement pour Lambda Web Functions
- Cycle de vie des environnements d'exécution
- Runtimes des fonctions Web Lambda
- Configuration des fonctions Web Lambda
- Autorisations relatives à la fonction Web Lambda
- Contrôle d'accès aux terminaux Lambda Web Function
- Chiffrement au repos pour les fonctions Web

- Surveillance des fonctions Web Lambda
- Exemples d'applications Web Function
- Bonnes pratiques pour les fonctions Web Lambda
- Test des fonctions Web Lambda
- Résolution des problèmes liés aux fonctions Web Lambda

Quand utiliser les fonctions Web

Utilisez les fonctions Web pour les charges de travail qui reçoivent et répondent directement au trafic HTTP. Cas d'utilisation courants :

- Applications Web : déployez des applications frontales ou complètes qui fournissent du HTML, des ressources et des itinéraires d'API à partir d'un seul déploiement.
- API REST et GraphQL : créez des backends d'API qui répondent à des volumes de requêtes élevés.
- Microservices : exécutez des services HTTP qui évoluent indépendamment du trafic, y compris jusqu'à zéro en cas d'inactivité.
- Server-side rendu (SSR) — Servez les pages qui sont affichées sur le serveur au moment de la demande plutôt que prédéfinies. Une fonction Web exécute directement le serveur de production de votre framework. Il gère les requêtes SSR, le streaming et les itinéraires d'API sans couche d'hébergement séparée. Il évolue également en fonction du trafic. Cela convient aux applications qui affichent un contenu personnalisé ou qui change fréquemment à chaque demande.
- Réponses en streaming : diffusez les résultats vers le client au fur et à mesure qu'ils sont produits, tels que les réponses provenant d'un grand modèle de langage.

Pour le traitement piloté par les événements, tel que la gestion des messages de file d'attente ou des téléchargements de fichiers, utilisez plutôt les fonctions d'événement Lambda.

> **Note**
>
> AWS Lambda Les fonctions Web ne prennent actuellement en charge que les Node.js environnements d'exécution. Si vous utilisezJava, Python.NET, ou un autre langage, reportez-vous the section called “Création de votre première fonction” à AWS Lambda Event Functions ou MicroVM à Lambda MicroVMS.

Fonctionnement des fonctions Web

Une fonction Web contient des révisions et des points de terminaison. Une révision est un instantané immuable de votre code et de votre configuration. Un point de terminaison achemine les requêtes HTTP vers une ou deux révisions. Lambda exécute votre serveur dans des environnements d'exécution qui gèrent chacun plusieurs requêtes simultanées. Lambda adapte ces environnements d'exécution en fonction du trafic. Pour plus de détails, consultez the section called “Concepts de base”.

Principaux avantages

Les fonctions Web offrent les avantages suivants pour les applications Web et les backends d'API :

- Expérience de développement Web standard : déployez Node.js des applications standard qui écoutent sur un port. Vous utilisez des frameworks Web familiers et votre structure d'application normale.
- Dimensionnement adaptatif : chaque environnement d'exécution répond à plusieurs demandes simultanées, comme un serveur Web standard. Par conséquent, un nombre réduit d'environnements d'exécution gèrent davantage de trafic. Les environnements d'exécution existants peuvent absorber de légères augmentations de trafic, de sorte que moins de demandes attendent le démarrage d'un nouvel environnement d'exécution.
- Usage-based facturation : vous payez pour les demandes, le temps processeur que votre application et votre environnement d'exécution consomment activement, la mémoire pendant la durée de vie de chaque environnement d'exécution et le transfert de données. Une requête en attente d'une requête de base de données ou d'un appel d'API externe consomme peu de CPU pendant son attente. Cependant, la mémoire continue de s'accumuler tant que l'environnement d'exécution existe, y compris le temps d'inactivité entre les demandes.
- Streaming des réponses : diffusez les réponses aux clients au fur et à mesure que votre application les produit, sans configuration supplémentaire.
- Échelle jusqu'à zéro : Lambda supprime les environnements d'exécution inactifs lorsqu'il n'y a pas de trafic et en crée de nouveaux lorsque les demandes arrivent. Une demande peut attendre l'initialisation d'un environnement d'exécution. Pour plus de détails sur le fonctionnement de la mise à l'échelle et de la régulation, voir. the section called “Mise à l’échelle”
- Built-in Point de terminaison HTTPS : chaque point de terminaison fournit un domaine HTTPS avec TLS. Vous choisissez l'authentification IAM ou l'authentification gérée par application pour chaque point de terminaison. Pour plus de détails, consultez the section called “Contrôle d’accès”. Pour

utiliser un domaine ou une AWS WAF protection personnalisés, placez une CloudFront distribution Amazon devant le point de terminaison.

- Endpoint-level contrôles du trafic — Définissez une limite de débit de demandes (demandes par seconde) sur chaque point de terminaison HTTPS, que Lambda applique dans chaque région, ainsi qu'un nombre maximum d'environnements d'exécution (`maxEnvironments`), également appliqués dans chaque région. Ensemble, ils vous permettent de limiter le trafic accepté par un point de terminaison. Ils vous permettent également de limiter la charge que le point de terminaison transmet aux dépendances en aval, telles que les bases de données et les API externes. Pour plus d'informations, consultez the section called “Mise à l’échelle”.

Concepts de base

La compréhension des concepts fondamentaux suivants vous permet de déployer et de gérer efficacement les applications Web. Cette page décrit le modèle de ressource d'une fonction Web, les états du cycle de vie de chaque ressource et la manière dont Lambda gère les requêtes HTTP entrantes.

Le modèle de ressource définit la structure d'une fonction Web. Une fonction Web est la ressource de premier niveau. Il contient des révisions (instantanés immuables de votre code et de votre configuration) et des points de terminaison (points d'entrée réseau qui acheminent le trafic HTTP vers vos révisions).

Les états de révision et les états des points de terminaison suivent la progression de ces ressources au fur et à mesure que Lambda les crée, les déploie et les supprime. La surveillance de ces états vous indique quand Lambda a fini de créer, de déployer ou de supprimer une ressource et vous aide à diagnostiquer les défaillances.

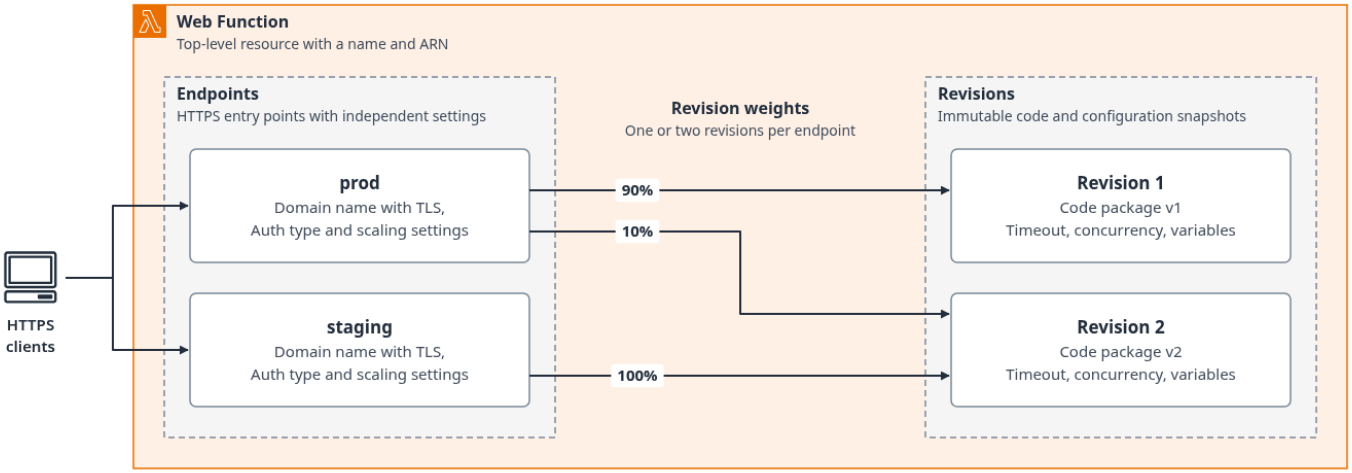
Les environnements d'exécution sont les instances de calcul isolées dans lesquelles s'exécutent votre serveur Web et votre application. Chaque environnement d'exécution gère plusieurs requêtes HTTP simultanées. Lambda crée et supprime des environnements automatiquement en fonction de la configuration et du trafic de votre fonction Web.

Les sections suivantes fournissent des informations détaillées sur chaque concept de base.

Modèle de ressources

Une fonction Web Lambda se compose de trois types de ressources dans une hiérarchie parent-enfant. La fonction Web est la ressource de premier niveau. Les révisions et les points de terminaison

sont des ressources dérivées de la fonction Web. Le déploiement du code ou la modification de la configuration des révisions créent une nouvelle révision. Le schéma suivant montre une fonction Web dont les points de terminaison acheminent le trafic vers ses révisions.



Fonction Web

La ressource de niveau supérieur qui représente votre application Web. Une fonction Web possède un nom, un ARN et son propre état de cycle de vie (en attente, active, en échec ou en suppression). Il peut contenir des révisions et des points de terminaison ; toutes les révisions et points de terminaison appartiennent à une seule fonction Web parente.

Révision

Un instantané immuable du code et de la configuration de votre application. Vous créez une nouvelle révision chaque fois que vous modifiez votre code ou la configuration de révision, par exemple le délai d'expiration des demandes, le nombre maximum de demandes simultanées par environnement d'exécution ou les variables d'environnement. Les révisions étant immuables, vous pouvez toujours revenir à une version précédente de votre application en acheminant le trafic vers une version antérieure. Vous pouvez répartir le trafic entre deux révisions à la fois pour les déploiements Canary ou Blue-Green.

Point de terminaison

Point d'entrée réseau qui achemine le trafic HTTP vers vos révisions. Chaque point de terminaison possède un nom de domaine unique avec TLS, un type d'authentification qui contrôle l'accès et des paramètres de dimensionnement qui définissent la capacité. Lorsque vous créez un point de terminaison, vous choisissez son type de point de terminaison, qui définit son étendue géographique. HomeRegiondessert uniquement le trafic provenant de la région d'origine. MultiRegiongère le trafic provenant de plusieurs régions via un domaine mondial,

qui achemine chaque demande vers une région en fonction de la latence du réseau, dans la mesure du possible. PerRegiongère le trafic provenant de plusieurs régions, chacune ayant son propre domaine régional, et vous contrôlez la manière dont les clients accèdent à chaque région. Une fonction Web peut avoir plusieurs points de terminaison, chacun ayant une configuration indépendante. Vous configurez les pondérations de révision sur un point de terminaison pour acheminer le trafic vers une ou deux révisions actives.

États de révision

Une révision passe par les états suivants au cours de son cycle de vie. Vous pouvez vérifier l'état actuel en appelant `GetWebFunctionRevision` ou en consultant les détails de la révision dans la console Lambda.

State	Description	Quelle est l'étape suivante ?
En suspens	Lambda est en train de créer la révision. Cela inclut le télécharg ement de votre code depuis Amazon S3 et la validation de la configuration.	La révision passe à Active lorsque la création est réussie, ou à Failed en cas d'erreur.
Actif	La révision a été créée avec succès et est prête à être placée derrière un point de terminaison.	La révision reste active jusqu'à ce que vous la supprimiez, que Lambda la supprime lors du nettoyage automatique des révisions (voirthe section called “Limites de révision et nettoyage automatique”) ou que vous supprimiez l'accès au code source. Si Lambda perd l'accès au code, par exemple parce que la version de l'objet Amazon S3 référencé a été supprimée, la révision passe au statut Failed (voirthe section called “Cycle de vie des objets”).
Échec	Lambda n'a pas pu créer la révision. Les problèmes détectés par Lambda lorsque vous soumettez la demande	Vérifiez le `stateReason` champ dans la `GetWebFunctionRevi sion` réponse pour plus de détails.

State	Description	Quelle est l'étape suivante ?
	ne produisent pas d'échec de révision. Par exemple, si les autorisations de la AWS KMS clé sont insuffisantes, la demande échoue avec une exception client et Lambda ne crée pas de révision.	Créez une nouvelle révision pour résoudre le problème. Les révisions ayant échoué ne peuvent pas desservir le trafic.

États de point de terminaison

Un point de terminaison possède deux champs d'état : `state` suit le cycle de vie global et `updateStatus` suit les mises à jour du point de terminaison après sa création initiale. Vous pouvez vérifier les deux en appelant`GetWebFunctionEndpoint`.

State	Description	Quelle est l'étape suivante ?
En suspens	Lambda est en train de créer le point de terminaison. Cela inclut l'attribution d'un nom de domaine, le provisionnement du protocole TLS et la configuration du routage. Pour les `PerRegion` terminaux `MultiRegion` et les terminaux , cela inclut également la réplication de la configuration vers d'autres. Régions AWS	Le point de terminaison passe à Actif lorsque la création réussit dans toutes les régions cibles, ou à Failed en cas d'erreur.
Actif	Le point de terminaison est prêt à recevoir du trafic HTTP sur son nom de domaine. Les clients peuvent envoyer des demandes au point de terminaison.	Le point de terminaison reste actif. Lambda suit les mises à jour ultérieures du point de terminaison `updateStatus` sur le terrain sans modifier l'état général du point de terminaison.
Échec	La création a échoué. Pour les `PerRegion` terminaux `MultiRegi`	Consultez le `stateReason` champ pour plus de détails. Pour les

State	Description	Quelle est l'étape suivante ?
	on et les terminaux, cela peut indiquer une défaillance dans une ou plusieurs régions cibles.	points de `PerRegion` terminais on `MultiRegion` et les points de terminaison, vérifiez les `regionalE ndpoints` entrées pour le `state` et `stateReason` pour chaque région.
Suppression en cours	Lambda supprime le point de terminaison et retire son nom de domaine. Pour les points `MultiRegi` on de `PerRegion` terminaison et les points de terminaison, Lambda supprime le point de terminaison de toutes les régions.	Une fois la suppression terminée, le point de terminaison est définitiv ement supprimé. Son nom de domaine est retiré et Lambda ne l'attribue jamais à un autre point de terminaison dans aucun compte. Cette opération ne peut pas être annulée.

Pour un point de terminaison existant, Lambda reste `state` défini sur `Active` lors d'une mise à jour du point de terminaison. Vérifiez si la mise `updateStatus` à jour la plus récente est `InProgressSuccessful`, ou`Failed`. Par exemple, lorsque vous modifiez les pondérations de révision d'un point de terminaison, `updateStatus` c'est `InProgress` pendant votre `state` séjour`Active`. Lorsque les nouvelles pondérations sont en vigueur, `updateStatus` passe à`Successful`.

InProgress

Lambda applique la mise à jour du point de terminaison.

Réussite

La dernière mise à jour du terminal est terminée et est en vigueur.

Échec

La dernière mise à jour du terminal a échoué. Vérifiez le `updateStatusReason` champ `regionalEndpoints` pour plus de détails. Pour les points de `PerRegion` terminaison `MultiRegion` et les points de terminaison, certaines régions peuvent utiliser la configuration précédente tandis que d'autres régions utilisent la configuration demandée. Corrigez la cause

signalée, puis appelez `UpdateWebFunctionEndpoint` à nouveau avec la configuration prévue pour réconcilier le point de terminaison.

L'état de la fonction Web, les états de révision et les états des points de terminaison sont indépendants. Une fonction Web peut être active alors que l'un de ses points de terminaison est toujours en attente ou a échoué. De même, une révision peut être active même si aucun point de terminaison n'achemine actuellement le trafic vers elle.

Une révision active, un point de terminaison actif ou une mise à jour réussie du point de terminaison ne confirment pas le démarrage de votre serveur. Lambda ne vérifie pas que votre serveur écoute lorsqu'il crée ou met à jour un point de terminaison pour utiliser une révision. Après chaque déploiement, envoyez une demande de test et consultez les journaux de votre application.

Environnements d'exécution

Un environnement d'exécution est une instance de calcul isolée dans laquelle s'exécutent votre serveur Web et votre application. Lorsque le trafic atteint votre point de terminaison, Lambda achemine les demandes vers les environnements d'exécution qui exécutent le code de la révision active.

Lambda gère automatiquement les environnements d'exécution :

1. Augmenter le volume : lorsque le trafic augmente, Lambda crée des environnements d'exécution supplémentaires et démarre votre serveur HTTP dans chacun d'eux. Lambda adapte les nouveaux environnements en avance sur la demande afin de conserver une marge de manœuvre. Les demandes attendent donc rarement le démarrage d'un nouvel environnement (démarrage à froid). Lorsqu'une fonction Web est mise à l'échelle à partir de zéro (la première requête après une période sans trafic), il y a un bref délai de démarrage à froid pendant que Lambda crée un environnement d'exécution. La demande attend que l'environnement d'exécution s'initialise. La demande peut toujours échouer si votre application ne démarre pas ou si un taux de demande, un environnement d'exécution ou une limite de compte s'appliquent. Pour plus de détails, consultez the section called “Mise à l’échelle”.
2. Diminution : lorsque le trafic diminue, Lambda supprime les environnements d'exécution dont il n'a plus besoin, une fois que les demandes en cours ont été traitées dans les meilleures conditions. Lambda s'adapte à zéro dans les environnements où il n'y a pas de trafic.

Le nombre d'environnements d'exécution et leur simultanéité sont contrôlés par deux paramètres :

- **`maxEnvironments`**(paramètre du point de terminaison) : nombre maximal d'environnements d'exécution que Lambda peut créer pour le point de terminaison dans chaque région. Ce paramètre est facultatif. Lorsqu'il n'est pas défini, Lambda adapte les environnements d'exécution selon les besoins, en fonction des quotas de votre compte.
- **`maxConcurrencyPerEnvironment`**(paramètre de révision) — Le nombre maximum de requêtes HTTP qu'un seul environnement d'exécution gère simultanément. Les valeurs valides sont comprises entre 1 et 128. La valeur par défaut est 64.

Lambda définit une limite de simultanéité dynamique pour chaque environnement d'exécution. Cette limite ne dépasse jamais`maxConcurrencyPerEnvironment`. La limite supérieure pour la simultanéité des terminaux est `maxEnvironments` multipliée par cette limite dynamique. La capacité réelle peut être inférieure car Lambda ajuste la simultanéité par environnement en fonction de l'utilisation des ressources et applique les limites des terminaux et des comptes. Supposons, par exemple, que vous ayez défini `maxEnvironments` la valeur 20 et `maxConcurrencyPerEnvironment` la valeur 64. Le point de terminaison gère ensuite jusqu'à 1 280 demandes simultanées dans une région. Il en gère moins si Lambda définit la limite dynamique en dessous de 64. Pour obtenir des conseils sur ces paramètres, consultez the section called “Mise à l’échelle”.

Traitement des demandes

Le code de votre fonction Web s'exécute comme un serveur HTTP standard qui écoute sur un port. Lambda envoie des requêtes HTTP entrantes à votre serveur et renvoie les réponses aux clients. Vous pouvez utiliser n'importe quel framework Node.js Web, intergiciel ou routeur.

Le cycle de vie des demandes fonctionne comme suit :

1. Un client envoie une requête HTTP au nom de domaine du point de terminaison.
2. Lambda authentifie la demande (pour les points de IamAuthterminaison) ou la transmet (pour les points de terminaison). ApplicationManaged
3. Lambda achemine la demande vers un environnement d'exécution en fonction des poids de révision du point de terminaison.
4. Le serveur HTTP de l'environnement d'exécution traite la demande et renvoie une réponse.
5. Lambda renvoie la réponse au client.

Chaque demande peut être exécutée pendant un maximum de 900 secondes (15 minutes). Vous pouvez configurer le délai d'attente de 3 à 900 secondes en utilisant le `timeoutSeconds` paramètre de révision. Le délai d'attente par défaut est de 30 secondes.

Chaque environnement d'exécution de fonction Web gère plusieurs demandes simultanées. Le code de votre application doit donc être sûr pour une utilisation simultanée. Pour plus de détails sur le modèle de simultanéité, voirthe section called “Node.js modèle d'exécution”.

Gestion des révisions des fonctions Web

Une révision est un instantané immuable du code et de la configuration de votre application Web Function. Pour modifier votre code ou tout paramètre de révision, par exemple `timeoutSecondsmaxConcurrencyPerEnvironment`, ou`environmentVariables`, vous créez une nouvelle révision. La réception du trafic par la nouvelle révision dépend du mode de déploiement automatique de chaque point de terminaison. Un point de terminaison en LatestRevisionmode achemine tout le trafic vers la nouvelle révision une fois celle-ci devenue active. Un point de terminaison en mode Disabled conserve ses pondérations de révision actuelles jusqu'à ce que vous les modifiiez. Les révisions étant immuables, vous pouvez revenir en arrière en acheminant le trafic vers une révision antérieure. La version précédente doit rester active, et son code, sa clé, son rôle et ses autres dépendances doivent rester disponibles. Pour plus d'informations sur le routage du trafic entre les révisions, consultezthe section called “Modèles de déploiement”.

Propriétés de révision

Chaque révision contient la configuration suivante :

Propriété	Description	Par défaut	Modifiable
RevisionID	ID unique généré par Lambda lorsque vous créez la révision.	–	Non (généré)
Révision ARN	Le nom de ressource Amazon (ARN) de la révision.	–	Non (généré)
Fonction ARN	L'ARN de la fonction Web à laquelle appartient la révision.	–	Non (généré)

Propriété	Description	Par défaut	Modifiable
state	État du cycle de vie de la révision (`Pending`Active, ou`Failed`). Pour plus de détails, consultez the section called “États de révision”.	–	Non (géré par Lambda)
STATEREASON	Description de la raison pour laquelle la révision est dans son état actuel, par exemple la cause d'un `Failed` état.	–	Non (géré par Lambda)
erreurs	Liste des erreurs détectées par Lambda lors de la création ou de la lecture de la révision. Chaque erreur nomme l'attribut concerné et inclut un code d'erreur et un message. Absent lorsque la révision ne comporte aucune erreur.	–	Non (géré par Lambda)
Créé à CreatedAt	Horodatage de création de la révision.	–	Non (généré)
description	Description facultative de la révision que vous fournissez lors de sa création.	Aucune	Non (immuable)
Config de construction	Le code et le runtime de la révision. Contient les `runtimeConfig` paramètres `codeConfig` et décrits dans les lignes suivantes.	–	Non (immuable)
Configuration du code	Emplacement du package de déploiement. Contient le `s3Object` paramètre décrit dans les lignes suivantes. Fait partie de`buildConfig` .	–	Non (immuable)

Propriété	Description	Par défaut	Modifiable
Objet S3	L'emplacement Amazon S3 du package de déploiement. Contient les `versionId` paramètres `bucketkey`, et décrits dans les lignes suivantes . Pour plus de détails, consultez the section called “Code dans Amazon S3”. Fait partie `decodeConfig` .	–	Non (immuable)
bucket	Nom du compartiment Amazon S3 qui contient le package de déploiement. La gestion des versions S3 doit être activée sur le compartiment. Fait partie `des30bject`.	–	Non (immuable)
key	La clé d'objet Amazon S3 du package de déploiement. Fait partie `des30bject`.	–	Non (immuable)
VersionID	L'ID de version de l'objet Amazon S3. Facultatif. Si vous l'omettez, Lambda utilise la dernière version de l'objet au moment de sa création. Quoi qu'il en soit, Lambda associe la révision à une version d'objet spécifique. Fait partie `des30bject`.	Dernière version	Non (immuable)
RuntimeConfig	La configuration d'exécution. Contient le `runtime` paramètre décrit dans la ligne suivante. Fait partie `debuildConfig` .	–	Non (immuable)

Propriété	Description	Par défaut	Modifiable
runtime	L'identifiant d'exécution (par exemple,`nodejs24.x`). Pour les environnements d'exécution pris en charge, consultezthe section called “Runtimes ”. Bien que l'identifiant d'exécution soit fixe pour la révision, le temps d'exécution lui-même n'est pas gelé. Lambda applique automatiquement des correctifs de sécurité et des corrections de bogues au moteur d'exécution, de sorte que l'identifiant (par exemple`nodejs24.x`) corresponde toujours à la dernière version corrigée. Pour plus de détails, consultez the section called “Correctif automatique lors de l'exécution”. Fait partie de`runtimeConfig` .	–	Non (immuable)
Configuration du service	Les paramètres d'exécution de la révision. Contient les `telemetryConfig` paramètres `executionRoleArn` `timeoutSeconds` ,`maxConcurrencyPerEnvironment` ,`environmentVariables` , et décrits dans les lignes suivantes.	–	Non (immuable)
exécution RoleArn	L'ARN du rôle IAM assumé par la fonction Web lors de l'exécution. Le rôle accorde des autorisations pour accéder aux AWS services et aux ressources. Obligatoire. Pour plus de détails, consultez the section called “Rôle d'exécution”. Fait partie de`serviceConfig` .	–	Non (immuable)

Propriété	Description	Par défaut	Modifiable
TimeOutSeconds	Durée maximale en secondes pendant laquelle une seule requête HTTP peut être exécutée. Valeurs valides : 3 à 900. Fait partie de `serviceConfig` .	30	Non (immuable)
maxConcurrencyPerEnvironment	Le nombre maximal de requêtes HTTP simultanées par environnement d'exécution. Valeurs valides : 1 à 128. Fait partie de `serviceConfig` .	64	Non (immuable)
Variables d'environnement	Key-value paires disponibles pour votre application au moment de l'exécution. Défini par révision et immuable après la création. Fait partie de `serviceConfig` .	Aucune	Non (immuable)
Configuration de télémétrie	Paramètres de télémétrie pour la révision. Contient le `loggingConfig` paramètre décrit dans les lignes suivantes. Si vous omettez `telemetryConfig` , Lambda envoie toujours les journaux de votre application au groupe de journaux par défaut. Fait partie de `serviceConfig` .	Aucune	Non (immuable)
Configuration de journalisation	Configuration de journalisation pour la révision. Contient les `systemLogLevel` paramètres `logGroup` `applicationLogLevel` , et décrits dans les lignes suivantes . Pour plus de détails, consultez the section called “Contrôles de journalisation”. Fait partie de `telemetryConfig` .	Aucune	Non (immuable)

Propriété	Description	Par défaut	Modifiable
LogGroup	Le groupe de CloudWatch journaux Amazon Logs qui reçoit vos journaux. Les noms de groupes de journaux commençant par `aws/` sont réservés et rejetés. Pour plus de détails, consultez the section called “Utilisation d'un groupe de journaux personnalisé”. Fait partie de `loggingConfig` .	`/aws/lambda/web/`*`functi name`*	Non (immuable)
applicationLogLevel	La sévérité minimale des journaux de votre application que Lambda envoie à Amazon CloudWatch Logs. Valeurs valides : `TRACE`, `DEBUG`, `INFO`, `WARN`, `ERROR`, et `FATAL`. Fait partie de `loggingConfig` .	`INFO`	Non (immuable)
système LogLevel	La sévérité minimale des journaux Lambda-generated système que Lambda envoie à Amazon CloudWatch Logs. Valeurs valides : `DEBUG`, `INFO` et `WARN`. Fait partie de `loggingConfig` .	`INFO`	Non (immuable)
kms KeyArn	L'ARN de la clé gérée par le client utilisée pour chiffrer le code et les variables d'environnement. Facultatif. Si un `MultiRegion` point de `PerRegion` terminaison achemine le trafic vers la révision, utilisez une clé multirégionale avec une réplique dans chacune des régions du point de terminaison. Pour plus de détails, consultez the section called “Chiffrement au repos”.	Aucune	Non (immuable)

Toutes les propriétés de révision sont immuables après leur création. Pour modifier une configuration, créez une nouvelle révision avec les valeurs mises à jour.

Création d'une révision

Lambda crée une révision lorsque vous appelez. `CreateWebFunctionRevision` Vous indiquez l'emplacement et la configuration du code dans la demande. Une nouvelle révision ne copie pas les paramètres d'une révision existante. Spécifiez tous les paramètres que vous souhaitez conserver, y compris les variables d'environnement. Les paramètres que vous omettez utilisent leurs valeurs par défaut. Pour commencer à partir des valeurs actuelles, `get-web-function-revision` exécutez-les et `buildConfig` réutilisez-les `serviceConfig` avec vos modifications. La nouvelle révision commence à l'état En attente pendant que Lambda télécharge votre code et prépare un artefact de code à partir de celui-ci. Lorsque la préparation est terminée, la révision passe à Active. Si une erreur se produit lors de la préparation, la révision passe en échec et ne peut pas desservir le trafic. Pour plus de détails sur chaque État, voirthe section called “États de révision”.

Avant de créer une révision, téléchargez votre package de déploiement .zip dans un compartiment Amazon S3 versionné et obtenez l'ARN d'un rôle d'exécution que Lambda peut assumer. Pour plus d’informations, consultez the section called “Code dans Amazon S3” et the section called “Rôle d'exécution”.

Pour créer une révision avec du code mis à jour (AWS CLI)

1. Exécutez la commande suivante pour créer une nouvelle révision. Remplacez le compartiment S3, la clé, l'ARN du rôle et les valeurs de configuration par les vôtres.

```
aws lambda-web create-web-function-revision \
    --function-name my-web-app \
    --build-config '{
      "codeConfig": {
        "s3Object": {
          "bucket": "my-bucket",
          "key": "my-app-v2.zip"
        }
      },
      "runtimeConfig": { "runtime": "nodejs24.x" }
    }' \
    --service-config '{
      "executionRoleArn": "arn:aws:iam::111122223333:role/my-web-function-role"
    }'
```

La commande utilise les objets suivants. Pour chaque paramètre et sa valeur par défaut, voirthe section called “Propriétés de révision”.

- `buildConfig`contient `codeConfig` le compartiment Amazon S3 et la clé de votre package de déploiement`runtimeConfig`, ainsi que le moteur d'exécution (par exemple,`nodejs24.x`). Ces deux noms sont requis.
- `serviceConfig`contient l'ARN requis `executionRoleArn` du rôle d'exécution assumé par votre fonction Web lors de son exécution. Il peut également contenir `timeoutSecondsmaxConcurrencyPerEnvironment`,`environmentVariables`, et`telemetryConfig`.

La commande renvoie des détails sur la nouvelle révision, y compris sa`revisionId`. La révision commence à l'état En attente.

2. Pour vérifier que la révision est active, exécutez la commande suivante. *`my-web-app`*Remplacez-le par le nom de votre fonction et *`rev-a1b2c`* par celui `revisionId` de la réponse.

```
aws lambda-web get-web-function-revision \
    --function-name my-web-app \
    --revision-id rev-a1b2c
```

La révision sera prête quand elle `state` le seraActive. Dans `state` l'affirmative`Failed`, `stateReason` décrit la cause. Pour plus de détails, consultez the section called “États de révision”.

Juste après avoir créé une révision, c'`state`est généralement le cas`Pending`. Pour attendre que ce soit le `Active` cas, exécutez `aws lambda-web wait web-function-revision-active` avec les mêmes options.

Pour créer une révision avec une configuration mise à jour (AWS CLI)

1. Pour modifier la configuration sans modifier le code, spécifiez le même emplacement de code avec les nouveaux paramètres. L'exemple suivant modifie le délai d'attente à 60 secondes et ajoute une variable d'environnement.

```
aws lambda-web create-web-function-revision \
```

```
    --function-name my-web-app \
    --build-config '{
      "codeConfig": {
        "s3Object": {
          "bucket": "my-bucket",
          "key": "my-app-v2.zip"
        }
      },
      "runtimeConfig": { "runtime": "nodejs24.x" }
    }' \
    --service-config '{
      "executionRoleArn": "arn:aws:iam::111122223333:role/my-web-function-role",
      "timeoutSeconds": 60,
      "maxConcurrencyPerEnvironment": 32,
      "environmentVariables": {
        "DATABASE_URL": "my-database-endpoint",
        "LOG_LEVEL": "info"
      }
    }'
```

2. Pour vérifier que la révision est active, exécutez la commande suivante. *my-web-app*Remplacez-le par le nom de votre fonction et *rev-a1b2c* par celui `revisionId` de la réponse.

```
aws lambda-web get-web-function-revision \
    --function-name my-web-app \
    --revision-id rev-a1b2c
```

   La révision sera prête quand elle `state` le seraActive. Dans `state` l'affirmativeFailed, `stateReason` décrit la cause. Pour plus de détails, consultez the section called “États de révision”.

   Juste après avoir créé une révision, c'stateest généralement le casPending. Pour attendre que ce soit le `Active` cas, exécutez `aws lambda-web wait web-function-revision-active` avec les mêmes options.

Après avoir créé la révision, la manière dont le trafic l'atteint dépend du mode de déploiement automatique du terminal. Pour plus de détails, consultez the section called “Modèles de déploiement”.

Révisions des listes

Pour afficher toutes les révisions d'une fonction Web, utilisez la commande suivante :

```
aws lambda-web list-web-function-revisions \
    --function-name my-web-app
```

La réponse inclut l'identifiant, l'état, l'horodatage de création et le résumé de la configuration de chaque révision. Utilisez l'identifiant de révision lors de la mise à jour des pondérations de révision du point de terminaison ou lors de la suppression d'une révision.

Supprimer une révision

Vous pouvez supprimer une révision qui n'est plus nécessaire. La suppression d'une révision la supprime définitivement. Votre package de déploiement dans Amazon S3 n'est pas affecté.

> **Important**
>
> Vous ne pouvez pas supprimer une révision vers laquelle un point de terminaison achemine le trafic (une révision dont le poids n'est pas nul pour un point de terminaison). Supprimez la révision des poids de révision de chaque point de terminaison avant de la supprimer.

Pour supprimer une révision (AWS CLI)

- Exécutez la commande suivante pour supprimer une révision spécifique.

  ```
  aws lambda-web delete-web-function-revision \
      --function-name my-web-app \
      --revision-id rev-a1b2c
  ```

Limites de révision et nettoyage automatique

Lambda utilise 50 révisions par fonction Web comme cible de nettoyage automatique. La cible n'est pas ajustable. Dans la console Service Quotas, il apparaît sous la forme Révisions par fonction Web (`web-function-revisions-per-function`).

Il n'est pas nécessaire de supprimer les anciennes révisions pour respecter l'objectif de nettoyage. Lorsqu'une nouvelle révision devient active et que le nombre total de révisions dépasse l'objectif

de nettoyage, Lambda supprime automatiquement les révisions les plus anciennes qui ne sont pas utilisées. Une révision est utilisée lorsqu'un point de terminaison achemine le trafic vers celui-ci, y compris lorsqu'il est référencé n'importe où dans la `regionalEndpoints` propriété d'un point de `PerRegion` terminaison `MultiRegion` ou point de terminaison. Lambda ne supprime pas automatiquement une révision en cours d'utilisation ou la révision qui vient de devenir active. Le nettoyage est asynchrone. Le nombre de révisions peut temporairement dépasser 50 alors que les anciennes révisions sont toujours utilisées ou que le nettoyage est en cours. Une révision que vous supprimez de toutes les pondérations de révision, telle qu'une cible d'annulation, peut être supprimée par un nettoyage.

Vous pouvez également supprimer des révisions manuellement à tout moment. Pour la procédure, reportez-vous à la section précédente.

Le package de déploiement de chaque révision peut atteindre 512 Mo (décompressé). Étant donné que vous fournissez votre package de déploiement dans votre propre compartiment Amazon S3 et que Lambda référence votre code directement à partir du compartiment, il n'existe pas de quota de stockage de code distinct pour les fonctions Web. Pour plus de détails, consultez the section called “Code dans Amazon S3”.

Configuration des paramètres de révision

Toutes les configurations sont définies par révision et sont immuables après leur création. Pour modifier un paramètre, créez une nouvelle révision avec les valeurs mises à jour. Les paramètres suivants contrôlent le comportement d'exécution.

Pour le délai d'expiration des demandes et les paramètres des variables d'environnement, voir the section called “Timeout” et the section called “Variables d’environnement” inthe section called “Configuration des fonctions Web”.

Concurrence par environnement

Le `maxConcurrencyPerEnvironment` paramètre contrôle le nombre de requêtes HTTP qu'un seul environnement d'exécution gère simultanément. Les valeurs valides sont comprises entre 1 et 128. La valeur par défaut est 64.

Pour les I/O-bound applications (nombreuses demandes en attente d'appels de base de données ou de réseau), une valeur plus élevée maximise l'utilisation. Pour CPU-bound les applications, une valeur inférieure réduit les conflits. Pour plus d'informations, consultez the section called “Mise à l’échelle”.

Points de terminaison de la fonction Web Lambda

Un point de terminaison est une ressource enfant d'une fonction Web qui fournit un point d'entrée réseau pour le trafic HTTP. Chaque point de terminaison inclut un nom de domaine unique avec TLS et un type d'authentification. Il comporte également des paramètres relatifs à la portée géographique, à la mise à l'échelle, à la régulation et au routage du trafic. Une fonction Web peut avoir jusqu'à 10 points de terminaison, chacun ayant une configuration indépendante.

Les sections suivantes décrivent les types de points de terminaison, les noms de domaine, l'authentification et la réplication. Pour plus d'informations sur les paramètres de mise à l'échelle et de limitation, consultez. the section called “Mise à l’échelle” Pour plus d'informations sur les modes de déploiement automatique et le routage du trafic, consultezthe section called “Modèles de déploiement”.

Types de point de terminaison

Le type de point de terminaison détermine la manière dont Lambda déploie votre fonction Web Régions AWS et la manière dont le trafic y est acheminé. Vous choisissez le type de point de terminaison lorsque vous créez le point de terminaison. Le type de point de terminaison ne peut pas être modifié après sa création.

HomeRegion

Exécute votre fonction Web en une seule fois Région AWS. Lambda traite les demandes provenant de la région dans laquelle vous avez créé le point de terminaison. Lambda alloue un seul nom de domaine régional au point de terminaison.

HomeRegionÀ utiliser pour les applications qui ne nécessitent pas de disponibilité multirégionale ou lorsque vous souhaitez commencer par la configuration la plus simple.

MultiRegion

Exécute votre fonction Web en plusieurs fois Régions AWS. Vous spécifiez les régions cibles lorsque vous créez le point de terminaison. Lambda ajoute automatiquement la région d'origine. Le point de terminaison doit inclure au moins une autre région. Pour acheminer le trafic vers une révision, vous définissez les poids de révision du point de terminaison. Lambda réplique ensuite automatiquement votre code et votre configuration dans toutes les régions spécifiées. Lambda alloue un seul nom de domaine global. Il utilise un routage basé sur la latence pour envoyer chaque demande à la région qui fournit généralement la latence la plus faible à l'appelant. Lambda n'effectue pas de basculement basé sur l'état de santé.

Vous gérez la fonction Web à partir d'une seule région d'origine. Lambda gère la réplication vers les autres régions. Les clients se connectent à un seul nom de domaine.

MultiRegionÀ utiliser pour les applications globales qui nécessitent une faible latence pour les utilisateurs situés dans plusieurs zones géographiques.

PerRegion

Exécute votre fonction Web de manière multiple Régions AWS, avec un nom de domaine régional distinct dans chaque région. Vous spécifiez les régions cibles lorsque vous créez le point de terminaison. Lambda ajoute automatiquement la région d'origine. Le point de terminaison doit inclure au moins une autre région. Lambda configure automatiquement le point de terminaison dans chaque région spécifiée. Chaque région possède son propre nom de domaine indépendant.

Contrairement à Lambda MultiRegion, il n'effectue pas de routage automatique basé sur la latence. Vous gérez la manière dont le trafic atteint chaque domaine régional, par exemple avec votre propre politique de routage Route 53 ou une CloudFront distribution.

À utiliser PerRegionlorsque vous devez contrôler les décisions d'itinéraire par région, par exemple pour mettre en œuvre des restrictions géographiques, une logique de basculement personnalisée ou des politiques de Region-specific trafic.

Les régions et le type de point de terminaison ne peuvent pas être mis à jour après leur création. Pour les modifier, créez un nouveau point de terminaison avec la configuration que vous souhaitez, migrez le trafic vers le nom de domaine du nouveau point de terminaison, puis supprimez l'ancien point de terminaison.

Pour plus de détails sur la façon dont Lambda réplique votre fonction Web entre les régions et achemine le trafic, consultez. the section called “Multi-Region déploiement”

Nom de domaine

Lambda attribue un nom de domaine unique à chaque point de terminaison lorsque vous le créez. Les clients envoient des requêtes HTTPS à ce domaine pour appeler votre fonction Web. Le domaine prend en charge le protocole HTTPS et Lambda gère le certificat TLS du domaine. Vous ne créez, ne renouvelez pas ou ne gérez pas les certificats vous-même.

Le format du nom de domaine dépend du type de point de terminaison :

- HomeRegionet PerRegion— Chaque région possède un domaine au format :

```
domain-id.shard-id.lambda-web.region.on.aws
```

Exemple : `bcdfghjklmnpqrst.b7t.lambda-web.ap-northeast-3.on.aws`

- MultiRegion— Un domaine global unique au format :

```
domain-id.lambda-web.global.on.aws
```

Exemple : `bcdfghjklmn.lambda-web.global.on.aws`

Lambda utilise le routage basé sur la latence pour sélectionner une région pour chaque client.

Vous pouvez récupérer le nom de domaine à partir de la `GetWebFunctionEndpoint` réponse ou de la console Lambda une fois que le point de terminaison a atteint l'état actif.

> **Note**
>
> Les points de terminaison Web Function ne prennent pas en charge l'attachement direct d'un nom de domaine personnalisé. Les clients qui appellent le domaine du point de terminaison doivent utiliser le nom Lambda-allocated de domaine. Pour diffuser du trafic sur votre propre domaine, placez une CloudFront distribution Amazon devant le point de terminaison et utilisez le nom de Lambda-allocated domaine comme origine.

Type d’authentification

Le `authType` paramètre contrôle si Lambda authentifie les requêtes HTTP entrantes avant de les transmettre à votre application. Vous pouvez mettre à jour ce paramètre sur un point de terminaison existant.

ApplicationManaged

Lambda n'authentifie pas les demandes entrantes. Toutes les requêtes HTTP sont transmises directement à votre application. Vous êtes responsable de la gestion de l'authentification dans le code de votre application.

IamAuth

Lambda valide la signature de chaque demande. Signez les demandes avec AWS Signature Version 4 (SigV4) pour PerRegionles domaines HomeRegionet avec Signature Version 4a (SigV4a) pour un MultiRegiondomaine global. Seuls les appelants `lambda:InvokeWebFunctionEndpoint` autorisés peuvent invoquer le point de terminaison.

Pour plus de détails sur l'authentification, y compris CloudFront l'intégration et les politiques basées sur les ressources, consultez. the section called “Contrôle d’accès”

Auto-deployment mode

Le `autoDeploymentMode` paramètre contrôle si Lambda achemine automatiquement le trafic vers les nouvelles révisions chaque fois que vous déployez votre application. Vous pouvez mettre à jour ce paramètre sur un point de terminaison existant.

Si vous omettez de le faire `autoDeploymentMode` dans une demande d'API, la valeur par défaut est. `Disabled` La console Lambda et l'utilisation des `aws lambda-web deploy` commandes `LatestRevision` pour les nouveaux `HomeRegion` points de terminaison. `LatestRevision`n'est pris en charge que pour les `HomeRegion` points de terminaison, donc `MultiRegion` et les `PerRegion` points de terminaison l'utilisent toujours. `Disabled` Lors de l'utilisation`Disabled`, spécifiez `revisionWeights` ce total de 100.

LatestRevision

Lambda achemine automatiquement 100 % du trafic vers la dernière révision active. À utiliser pour les environnements de développement et de mise en scène. LatestRevision le mode n'est disponible que pour les HomeRegionpoints de terminaison.

Désactivé

Lambda ne modifie pas le routage du trafic lorsque vous créez une nouvelle révision. Vous contrôlez le routage manuellement à l'aide des pondérations de révision. À utiliser pour les environnements de production. Le mode désactivé est disponible pour tous les types de terminaux. MultiRegionet les PerRegionterminaux utilisent toujours le mode Disabled.

Pour plus de détails sur les modèles de déploiement, les annulations et le comportement de changement de mode, consultezthe section called “Modèles de déploiement”.

Mise à l'échelle et régulation

Chaque point de terminaison possède des paramètres de dimensionnement et de limitation qui contrôlent la capacité. Vous pouvez mettre à jour ces paramètres sur un terminal existant avec`update-web-function-endpoint`. Omettez `--scaling-config` ou `--throttle-config` conservez sa valeur actuelle, ou transmettez un objet vide (`'{}'`) pour effacer une valeur précédemment définie. Pour supprimer une limite de débit, transmettez un `--throttle-config` objet vide. A `rateLimit` de 0 bloque tout le trafic.

- **`maxEnvironments`** : facultatif. Le nombre maximum d'environnements d'exécution pour le point de terminaison dans chaque région. Lorsqu'il n'est pas défini, le point de terminaison évolue selon les besoins dans les limites des quotas du compte.
- **`rateLimit`**— Nombre maximum de demandes par seconde. Ce paramètre est facultatif. Lorsqu'il n'est pas défini, le point de terminaison est limité par le quota de 10 000 RPS par point de terminaison et par les quotas de compte. La limite de débit s'applique au point de terminaison dans son ensemble, dans tous les environnements d'exécution. Il ne s'agit pas d'une limite par environnement. Pour les points MultiRegionde PerRegionterminaison et les points de terminaison, chaque région applique la limite de manière indépendante. Les demandes excédentaires reçoivent le protocole HTTP 429.

Pour plus de détails sur la façon dont ces paramètres interagissent avec la simultanéité au niveau de la révision et pour obtenir des conseils sur le choix des valeurs, voir. the section called “Mise à l’échelle”

Création et gestion de points de terminaison

Création d’un point de terminaison

Pour créer un HomeRegion point de terminaison (AWS CLI)

- ```
  aws lambda-web create-web-function-endpoint \
      --function-name my-web-app \
      --endpoint-name my-endpoint \
      --endpoint-type HomeRegion \
      --auth-type ApplicationManaged \
      --auto-deployment-mode LatestRevision
  ```
  ```

Pour créer un MultiRegion point de terminaison (AWS CLI)

- ```
  aws lambda-web create-web-function-endpoint \
      --function-name my-web-app \
      --endpoint-name my-global-endpoint \
      --endpoint-type MultiRegion \
      --regions us-east-1 eu-west-1 ap-northeast-1 \
      --auth-type ApplicationManaged \
      --revision-weights '[{"revisionId": "rev-a1b2c", "weight": 100}]'
  ```

  MultiRegion et les PerRegion points de terminaison nécessitent des pondérations de révision, car LatestRevisionle déploiement automatique n'est pas disponible pour eux. Pour plus d'informations, consultez the section called “Modèles de déploiement”.

Répertorier les points de terminaison

```
aws lambda-web list-web-function-endpoints \
    --function-name my-web-app
```

La réponse inclut le nom, le type, le nom de domaine, l'état et la configuration de chaque point de terminaison.

Obtenir des informations sur les terminaux

```
aws lambda-web get-web-function-endpoint \
    --function-name my-web-app \
    --endpoint-name my-endpoint
```

La réponse inclut le nom de domaine, l'état, le type d'authentification, le mode de déploiement automatique, les paramètres de dimensionnement, les pondérations de révision et (pour `MultiRegion` et les `PerRegion` points de terminaison) l'état de chaque région et le statut de mise à jour sur le `regionalEndpoints` terrain.

Mise à jour d'un terminal

Vous pouvez mettre à jour les propriétés suivantes sur un point de terminaison existant :

- `description`
- `authType`
```

- `autoDeploymentMode`
- `revisionWeights`
- `scalingConfig`
- `throttleConfig`

Vous ne pouvez pas mettre à jour les propriétés suivantes. Pour les modifier, créez un nouveau point de terminaison avec la configuration que vous souhaitez, migrez le trafic vers le nom de domaine du nouveau point de terminaison, puis supprimez l'ancien point de terminaison.

- `endpointType` (HomeRegion, MultiRegion, PerRegion)
- `regions`(les régions cibles du terminal)

Suppression d'un point de terminaison

```
aws lambda-web delete-web-function-endpoint \
    --function-name my-web-app \
    --endpoint-name my-endpoint
```

Lorsque vous supprimez un point de terminaison, il passe à l'état Suppression. Lambda arrête de router les nouvelles demandes vers le point de terminaison et retire son nom de domaine. Pour un `PerRegion` point de terminaison, Lambda retire le nom de domaine dans chaque région. Lambda n'attribue jamais les noms de domaine d'un point de terminaison supprimé à un autre point de terminaison dans aucun compte. Lambda draine les demandes en vol. Il permet aux demandes déjà en cours de se terminer et rejette les nouvelles demandes adressées aux noms de domaine du point de terminaison. Pour les points `MultiRegion` de `PerRegion` terminaison et les points de terminaison, Lambda supprime le point de terminaison de toutes les régions. Une fois la suppression terminée, Lambda supprime définitivement le point de terminaison.

La suppression d'un point de terminaison n'entraîne pas la suppression de la fonction Web ni de ses révisions. Les révisions restent disponibles pour être utilisées par d'autres points de terminaison.

Création d'une fonction Web Lambda

Pour déployer une application avec Lambda Web Functions, vous devez créer une fonction Web avec une révision et un point de terminaison pour recevoir le trafic. La console et la `aws lambda-web deploy` commande peuvent créer la fonction Web, sa première révision et son premier point de

terminaison. Les révisions sont des instantanés immuables de votre code et de votre configuration. Un point de terminaison achemine les demandes vers une révision active. Pour plus d'information sur ces ressources, consultez the section called "Concepts de base". Cette rubrique explique comment les créer à l'aide de la console Lambda et du. AWS CLI

Conditions préalables

Avant de commencer, assurez-vous de disposer des éléments suivants :

- Un AWS compte. Pour en créer une, voir Comparer les options d'inscription dans le Guide de référence sur la gestion des AWS comptes.
- Autorisations permettant de gérer les fonctions Web, de transmettre le rôle d'exécution à Lambda (`iam:PassRole`) et de créer ou d'utiliser les ressources Amazon S3 et IAM associées.

La console crée ou réutilise les ressources dont votre fonction Web a besoin, notamment un rôle d'exécution et un compartiment Amazon S3 pour votre code.

Pour suivre la AWS CLI procédure, vous devez également :

- AWS CLI version 2, dans une version qui inclut les `aws lambda-web` commandes. Pour vérifier, courez`aws lambda-web help`. Si vous l'avez installé AWS CLI à l'aide d'un programme d'installation ou d'un script d'installation officiel, exécutez-le `aws update` pour effectuer la mise à jour vers la dernière version. Sinon, consultez la section Installation ou mise à jour vers la dernière version du AWS CLI.
- AWS des informations d'identification et une Région AWS configuration pour le AWS CLI.
- Pour`aws lambda-web deploy`, l'autorisation d'appeler`sts:GetCallerIdentity`, `s3:ListBucket` sur le compartiment de déploiement `s3:PutObjects3:GetObject`, et `s3:GetObjectVersion` sur ses objets.
- Si `aws lambda-web deploy` crée les ressources par défaut, l'autorisation d'appeler `iam:GetRoleiam:CreateRole`,`iam:PutRolePolicy`,`s3:CreateBucket`,`s3:PutBucketPolicy`, ets`3:PutBucketVersioning`.
- (Facultatif) Node.js 24 ou plus tard pour le développement local. Pour procéder à l'installationNode.js, consultez la section Téléchargement Node.js sur le Node.js site Web.

Création d'une fonction Web (console)

Utilisez la console Lambda pour créer une fonction Web, sa première révision et son premier point de terminaison à recevoir du trafic.

Pour créer une fonction Web et un point de terminaison (console)

1. Ouvrez la console Lambda à l'adresse. https://console.aws.amazon.com/lambda/
2. Dans le volet de navigation, sélectionnez Web Functions.
3. Choisissez Create Web Function.
4. Sous Basic information (Informations de base), procédez comme suit :
   a. Dans Nom de la fonction, entrez le nom de votre fonction Web.
   b. Pour Runtime, conservez le runtime par défaut.
   c. Pour le code source, conservez le modèle Hello World pour commencer à partir d'un exemple d'application préconfiguré. Pour déployer votre propre code à la place, choisissez Upload ZIP file ou Amazon S3.
5. Sous Configuration du point de terminaison, procédez comme suit :
   a. Dans Nom du point de terminaison, entrez un nom pour le point de terminaison.
   b. Pour Type, conservez Home-Region. Un Home-Region point de terminaison s'exécute dans une seule région, ce qui en fait la configuration la plus simple pour votre première fonction Web. Pour les options multirégionales, voirthe section called “Points de terminaison”.

      > **Note**
      > Vous ne pouvez pas modifier le type de point de terminaison après sa création.

   c. Pour Type d'authentification, choisissez Application-managed Authentification. Avec cette option, Lambda transmet toutes les demandes à votre application, afin que celle-ci gère l'authentification. Pour restreindre l'accès, choisissez plutôt l'authentification IAM, qui oblige les appelants à signer les demandes. Les demandes `HomeRegion` et les `PerRegion` points de terminaison utilisent AWS Signature Version 4 (SigV4). Les demandes adressées aux `MultiRegion` points de terminaison utilisent la version de signature 4a (SIGv4a). Pour plus d'informations, consultez the section called “Contrôle d'accès”.
   d. Pour le déploiement automatique, conservez la dernière révision. Avec ce mode, Lambda achemine automatiquement tout le trafic vers chaque nouvelle révision une fois qu'elle

est devenue active. Pour un contrôle manuel du trafic avec des pondérations de révision, choisissez Disabled. Pour plus d'informations, consultez the section called “Modèles de déploiement”.

6. (Facultatif) Développez les configurations supplémentaires pour remplacer les paramètres par défaut. Par défaut, Lambda crée un rôle d'exécution autorisé à télécharger des journaux sur Amazon CloudWatch, et un compartiment Amazon S3 dans votre compte pour stocker votre code. Dans cette section, vous pouvez choisir un rôle IAM existant ou votre propre compartiment Amazon S3, et vous pouvez également configurer le chiffrement avec une clé gérée par le client, la simultanéité maximale par environnement, les variables d'environnement et les balises.
7. Choisissez Create Web Function.

Lorsque vous choisissez Create Web Function, Lambda crée la ressource Web Function avec sa première révision, et crée le point de terminaison en même temps. La révision commence à l'état En attente pendant que Lambda télécharge votre code et prépare un artefact de code à partir de celui-ci, puis passe à Active. Le point de terminaison démarre également à l'état En attente. La fonction Web, sa révision et son point de terminaison progressent chacun dans ces états indépendamment. Pour plus d'informations sur les révisions et les états du cycle de vie, consultezthe section called “Concepts de base”.

Le point de terminaison commence à desservir le trafic lorsqu'il devient actif et qu'il existe une révision active vers laquelle il peut être acheminé. Pour trouver le nom de domaine du point de terminaison, sur la page détaillée de la fonction, choisissez l'onglet Points de terminaison, puis choisissez le point de terminaison. Pour diffuser l'application sur votre propre domaine, placez une CloudFront distribution Amazon devant le point de terminaison. Pour plus d'informations sur les types de points de terminaison et les noms de domaine, consultezthe section called “Points de terminaison”.

Pour vérifier que votre application diffuse du trafic, envoyez une demande au nom de domaine. Comme vous avez choisi Application-managed l'authentification, vous pouvez envoyer une simple demande sans la signer.

```
curl https://your-endpoint-domain-name/
```

Une réponse réussie signifie que votre fonction Web reçoit du trafic et que votre application répond aux demandes.

Création d'une fonction Web (AWS CLI)

Créez et déployez une fonction Web à partir de votre terminal. La commande de démarrage génère un petit serveur Node.js HTTP, le déploie et renvoie une URL de point de terminaison HTTPS.

Déployez et testez votre fonction Web

Pour déployer et tester une fonction Web de démarrage

1. Exécutez la commande suivante :

   ```
   aws lambda-web deploy --name my-web-app --hello-world
   ```

   `--hello-world`décrit les fichiers de démarrage dans le répertoire `./my-web-app`, en créant le répertoire s'il n'existe pas. Le starter contient `server.ts` un serveur TypeScript HTTP, et `package.json`README.md, et`AGENTS.md`.
2. Lorsque le déploiement est terminé, copiez l'URL du point de terminaison à partir de la sortie. L'URL ressemble à ce qui suit :

   ```
   https://bcdfghjklmnpqrst.b7t.lambda-web.us-east-1.on.aws
   ```
3. Envoyez une demande à l'URL du point de terminaison que vous avez copié à l'étape précédente. Remplacez *`endpoint-url`* par cette URL :

   ```
   curl endpoint-url
   ```

   Le starter renvoie une réponse similaire à la suivante :

   ```
   {"message":"Hello from Lambda Web!","path":"/"}
   ```

Par défaut, le point de terminaison de départ accepte les demandes sans authentification. Pour demander l'autorisation IAM, ajoutez`--auth-type IamAuth`. Pour plus d'informations sur le contrôle de l'accès à votre terminal, consultezthe section called “Contrôle d’accès”.

Ce que la commande crée

Lors du premier déploiement, la commande :

- Crée ou réutilise un compartiment Amazon S3 avec la gestion des versions activée pour les packages de déploiement.
- Crée ou réutilise un rôle d'exécution IAM avec les autorisations Amazon CloudWatch Logs.
- Crée la fonction Web et sa première révision.
- Crée un `HomeRegion` point de terminaison nommé `dev` et attend qu'il le devienne`Active`. Pour utiliser un autre nom, ajoutez`--endpoint-name`.

Une fonction Web contient des révisions immuables de votre code et de votre configuration. Lors des déploiements ultérieurs, la commande crée une autre révision. Le `dev` point de terminaison utilise le `LatestRevision` mode et diffuse la révision une fois qu'elle est devenue active.

Déployer une modification

Après avoir modifié l'application de démarrage, exécutez :

```
aws lambda-web deploy \
  --name my-web-app \
  --code ./my-web-app
```

L'exécution de cette commande télécharge votre package mis à jour, crée une révision et attend que la révision devienne effective. `Active` Le `dev` point de terminaison a `autoDeploymentMode` défini la révision `LatestRevision` et la diffuse automatiquement. Son URL reste la même.

Pour déployer votre propre application au lieu du starter, transmettez son répertoire à`--code`. Votre serveur doit écouter l'hôte et le port dans la variable d'`AWS_LAMBDA_HTTP_ENDPOINT`environnement. Par défaut, le moteur d'exécution `index.js` se charge à la racine du package de déploiement. Pour utiliser un autre fichier d'entrée, définissez la variable d'`AWS_LAMBDA_NODEJS_ENTRYPOINT`environnement. Lambda ne vérifie pas que votre serveur commence à écouter lorsqu'il crée la révision. Par conséquent, la révision et le point de terminaison peuvent s'afficher `Active` même si les demandes échouent. Pour plus d'informations, consultez the section called “Runtimes ”.

Utiliser l'existant AWS resources

Si vous gérez déjà un bucket Amazon S3 ou un rôle d'exécution IAM, utilisez la commande suivante pour réutiliser ces ressources au lieu de créer des valeurs par défaut. La gestion des versions du compartiment doit être activée et une politique de compartiment doit accorder le principal de service Lambda `lambda.amazonaws.com` () `s3:GetObject` et. `s3:GetObjectVersion` La commande

ne modifie pas la configuration d'un compartiment que vous spécifiez. Pour les exigences relatives aux compartiments, voirthe section called “Politique relative aux compartiments pour Lambda”. Remplacez les exemples de valeurs de ressources par les vôtres.

```
aws lambda-web deploy \
  --name my-web-app \
  --code ./my-web-app \
  --bucket-name amzn-s3-demo-bucket \
  --execution-role-arn arn:aws:iam::111122223333:role/my-web-app-execution-role
```

Le rôle d'exécution doit permettre à Lambda de l'assumer et doit accorder les autorisations dont votre application a besoin. Pour plus d’informations, consultez the section called “Rôle d'exécution”.

Vous pouvez omettre l'une ou l'autre des options de ressource pour permettre de `deploy` créer des valeurs par défaut. Lorsque vous `deploy` créez une fonction Web sans `--hello-world` point de terminaison ou que vous en ajoutez un, elle vous demande d'appuyer sur Entrée pour confirmer. Dans un script ou un CI/CD pipeline, ajoutez `--create` pour confirmer sans invite.

Utilisez directement les commandes de l'API

La `deploy` commande télécharge votre code sur Amazon S3 et crée la fonction Web, la révision et le point de terminaison pour vous. Pour contrôler vous-même chaque étape, utilisez les AWS CLI commandes associées aux opérations de l'API, telles que `create-web-function`create-web-function-revision, et`update-web-function-endpoint`. Dans les commandes suivantes, remplacez chaque espace réservé pour l’entrée utilisateur par vos propres informations.

Pour créer une fonction Web à l'aide des commandes de l'API (AWS CLI)

1. Créez un package de déploiement .zip à partir du répertoire de votre application, avec votre fichier d'entrée à la racine du package. Téléchargez le package dans un compartiment Amazon S3 répondant aux exigences dethe section called “Conditions préalables”. Les commandes suivantes créent le package et utilisent le AWS CLI pour le télécharger.

   ```
   cd my-app
   zip -r ../my-app.zip .
   aws s3 cp ../my-app.zip s3://amzn-s3-demo-bucket/my-app.zip
   ```

2. Utilisez la AWS CLI commande suivante pour créer la fonction Web avec sa première révision et son point de terminaison. Dans`revisionConfig`, `buildConfig` indique

l'emplacement du code et le temps d'exécution, ainsi `serviceConfig` que le rôle d'exécution. La `endpointConfig` propriété définit le point de terminaison.

```
aws lambda-web create-web-function \
    --function-name my-web-app \
    --revision-config '{
      "buildConfig": {
        "codeConfig": {
          "s3Object": { "bucket": "amzn-s3-demo-bucket", "key": "my-app.zip" }
        },
        "runtimeConfig": { "runtime": "nodejs24.x" }
      },
      "serviceConfig": {
        "executionRoleArn": "arn:aws:iam::111122223333:role/my-web-app-execution-
role"
      }
    }' \
    --endpoint-config '{
      "endpointName": "my-endpoint",
      "endpointType": "HomeRegion",
      "authType": "ApplicationManaged",
      "autoDeploymentMode": "LatestRevision"
    }'
```

La propriété `autoDeploymentMode` est facultative. Si vous l'omettez, la valeur par défaut est`Disabled`, et le point de terminaison n'achemine pas automatiquement le trafic vers les nouvelles révisions. Notez `revisionId` la version révisée dans la réponse.

3. Patientez jusqu'à ce que la révision soit terminée`Active`. *`rev-abc12`*Remplacez-le par l'ID de révision de l'étape précédente.

```
aws lambda-web wait web-function-revision-active \
    --function-name my-web-app \
    --revision-id rev-abc12
```

4. Obtenez les détails du point de terminaison.

```
aws lambda-web get-web-function-endpoint \
    --function-name my-web-app \
    --endpoint-name my-endpoint
```

Lorsque c'`state`est le cas du point de terminaison`Active`, envoyez des demandes à son`domainName`. La réponse ressemble à l'extrait suivant.

```
{
    "endpointName": "my-endpoint",
    "endpointType": "HomeRegion",
    "domainName": "bcdfghjklmnpqrst.b7t.lambda-web.us-east-1.on.aws",
    "authType": "ApplicationManaged",
    "autoDeploymentMode": "LatestRevision",
    "state": "Active",
    "updateStatus": "Successful"
}
```

Pour déployer une modification à l'aide des commandes de l'API (AWS CLI)

- Téléchargez un nouveau package et créez une révision. Une révision est un instantané complet, alors transmettez-le dans son intégralité `buildConfig` et à `serviceConfig` chaque fois.

```
aws s3 cp ../my-app.zip s3://amzn-s3-demo-bucket/my-app.zip
aws lambda-web create-web-function-revision \
    --function-name my-web-app \
    --build-config '{
      "codeConfig": {
        "s3Object": { "bucket": "amzn-s3-demo-bucket", "key": "my-app.zip" }
      },
      "runtimeConfig": { "runtime": "nodejs24.x" }
    }' \
    --service-config '{
      "executionRoleArn": "arn:aws:iam::111122223333:role/my-web-app-execution-
role"
    }'
```

Comme le point de terminaison est `autoDeploymentMode` défini sur`LatestRevision`, il achemine tout le trafic vers la nouvelle révision une fois celle-ci passée`Active`. Si vous définissez `autoDeploymentMode` cette option`Disabled`, vous acheminez le trafic avec des `update-web-function-endpoint` pondérations de révision à la place. Pour plus d'informations, consultez the section called “Modèles de déploiement”.

Nettoyage

Lorsque vous n'avez plus besoin de la fonction Web, supprimez-la :

```
aws lambda-web delete-web-function --function-name my-web-app
```

Cette commande supprime également les points de terminaison et les révisions de la fonction Web. Il ne supprime pas les ressources `deploy` créées ou utilisées : le rôle d'exécution IAM (`awscli-lambdaweb-my-web-app`par défaut), les packages de déploiement contenus `lambda-web/my-web-app/` dans le compartiment Amazon S3 (`awscli-lambdaweb-`*`account-id`*`-`*`region`*`-an`par défaut), y compris les versions d'objets non actuelles, ou les groupes de CloudWatch journaux Amazon Logs pour la fonction Web. Supprimez ces ressources séparément uniquement si vous n'en avez plus besoin. Le compartiment Amazon S3 géré peut être partagé par d'autres déploiements de la même Compte AWS région.

Déploiement de fonctions Web

Vous déployez une fonction Web en fournissant le code de votre application sous forme de package .zip dans un compartiment Amazon S3. Lorsque vous déployez une nouvelle révision, vous contrôlez la manière dont le trafic y est acheminé grâce à des modèles de déploiement tels que Canary et Blue-Green. Pour les applications globales, vous pouvez déployer plusieurs applications Régions AWS derrière un seul point de terminaison, et Lambda achemine chaque demande vers une région en fonction de la latence du réseau. Lambda ne garantit pas que chaque demande soit envoyée vers la région à latence la plus faible.

Rubriques

- Déploiement du code de fonction Web depuis Amazon S3
- Modèles de déploiement
- Multi-Region déploiement

Déploiement du code de fonction Web depuis Amazon S3

Vous fournissez le code Lambda Web Function sous forme de package de déploiement .zip dans un compartiment Amazon S3. C'est le seul moyen de fournir du code pour une fonction Web. Lorsque vous créez une fonction Web ou une révision, spécifiez l'objet dans le `s3Object` champ, qui est imbriqué dans `codeConfig` celui de `buildConfig` la demande. Dans`s3Object`, incluez le bucket,

la clé et un versionId facultatif. Lambda référence votre code directement depuis votre bucket. Comme Lambda associe chaque révision à une version d'objet spécifique, vos déploiements sont reproductibles. Vous pouvez réutiliser un seul package de déploiement entre les comptes et AWS les régions.

Rubriques

- Conditions préalables
- Autorisations requises
- Création d'une fonction Web avec du code provenant d'Amazon S3
- Cycle de vie des objets
- Multi-Region déploiements

Conditions préalables

Avant de déployer le code de fonction Web depuis Amazon S3, assurez-vous que votre compartiment et votre package de déploiement répondent aux exigences suivantes :

Versionnage S3

La gestion des versions S3 doit être activée sur le compartiment. Lambda utilise des versions d'objets pour savoir quelle version de votre code est utilisée par une révision.

ID de version

Le `versionId` paramètre est facultatif dans la demande. Si vous l'omettez, Lambda utilise la dernière version de l'objet au moment de sa création. Quoi qu'il en soit, Lambda associe la révision à une version d'objet spécifique.

Taille maximale du package de déploiement

512 Mo (décompressé).

Fichier d'entrée

Le package de déploiement doit contenir le fichier d'entrée de votre application. Par défaut, le moteur d'exécution `index.js` se charge à la racine du package. Pour utiliser un autre fichier d'entrée, définissez la variable d'`AWS_LAMBDA_NODEJS_ENTRYPOINT`environnement de la révision sur le chemin du fichier par rapport à la racine du package. Après avoir chargé le fichier d'entrée, le moteur d'exécution attend que votre serveur HTTP commence à écouter l'hôte et le port à partir de la variable d'`AWS_LAMBDA_HTTP_ENDPOINT`environnement. Si le moteur

d'exécution ne parvient pas à résoudre le fichier d'entrée ou si le serveur ne commence jamais à écouter, l'initialisation échoue et les demandes adressées au point de terminaison échouent.

Lambda ne vérifie pas que votre serveur commence à écouter lorsqu'il crée ou met à jour un point de terminaison pour utiliser la révision. La révision et le point final peuvent toujours s'afficher `Active` dans ces cas. Après chaque déploiement, envoyez une demande de test et consultez les journaux de votre application.

Emplacement du godet

Le bucket peut se trouver dans un AWS compte et dans une AWS région différents de ceux de la fonction Web. Le bucket doit se trouver dans la même AWS partition que la fonction Web. Le compartiment ne peut pas se trouver dans une région optionnelle (une région qui n'est pas activée par défaut). Si l'une des conditions n'est pas remplie, Lambda rejette la demande. Cross-Region la récupération d'objets entraîne des coûts de transfert de données supplémentaires sur Amazon S3. Pour plus d'informations sur la tarification, consultez Tarification Amazon S3.

Autorisations requises

Pour déployer le code de fonction Web depuis Amazon S3, vous devez configurer des autorisations pour l'identité d'appel et pour le principal de service Lambda.

Autorisations de l'appelant

Pour créer la fonction Web ou la révision, votre identité IAM a besoin des autorisations suivantes sur l'objet S3 :

- `s3:GetObject`
- `s3:GetObjectVersion`

Pour les buckets multicomptes, la politique des compartiments doit également accorder à l'identité appelante l'accès à l'objet.

Politique relative aux compartiments pour Lambda

La politique du bucket doit accorder le principal du service Lambda (`lambda.amazonaws.com`) `s3:GetObject` et les `s3:GetObjectVersion` autorisations. Définissez la politique avec une `aws:SourceArn` condition qui correspond au modèle ARN de révision. `ArnLike`À utiliser avec un caractère générique pour l'ID de révision, car Lambda génère l'ID de révision lorsque vous créez la révision.

Si l'objet est chiffré avec une AWS KMS clé (SSE-KMS), la politique des clés doit également `lambda.amazonaws.com` permettre `kms:Decrypt` d'appeler cette clé. Lambda vérifie l'accès du principal du service lorsque vous créez la révision et rejette la demande si l'accès est manquant.

L'exemple de politique de compartiment suivant accorde à Lambda l'accès pour lire vos packages de déploiement pour toute révision de la fonction Web spécifiée.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowLambdaWebFunctionCodeAccess",
            "Effect": "Allow",
            "Principal": {
                "Service": "lambda.amazonaws.com"
            },
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": "arn:aws:s3:::my-bucket/*",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:lambda:us-east-1:111122223333:web-
function/my-function/revision/*"
                }
            }
        }
    ]
}
```

Pour limiter l'accès au préfixe clé qui contient vos packages de déploiement, remplacez la `Resource` valeur par`arn:aws:s3:::my-bucket/my-prefix/*`, où *`my-bucket`* se trouvent le nom de votre bucket et *`my-prefix`* le préfixe clé. Conservez le `/*` à la fin du préfixe. Ne modifiez pas le `revision/*` joker. `aws:SourceArn`

Création d'une fonction Web avec du code provenant d'Amazon S3

Vous spécifiez votre package de déploiement S3 dans la `codeConfig` section de`buildConfig`. Les procédures suivantes montrent comment créer une fonction Web et comment créer une nouvelle révision à l'aide du AWS CLI.

Pour créer une fonction Web avec du code provenant d'Amazon S3 (AWS CLI)

- Exécutez la commande suivante pour créer une fonction Web qui fait référence à votre package de déploiement .zip dans Amazon S3.

```
aws lambda-web create-web-function \
    --function-name my-web-app \
    --revision-config '{
      "buildConfig": {
        "codeConfig": {
          "s3Object": { "bucket": "my-bucket", "key": "my-app.zip" }
        },
        "runtimeConfig": { "runtime": "nodejs24.x" }
      },
      "serviceConfig": {
        "executionRoleArn": "arn:aws:iam::111122223333:role/my-web-function-role"
      }
    }' \
    --endpoint-config '{
      "endpointName": "my-endpoint",
      "endpointType": "HomeRegion",
      "authType": "ApplicationManaged"
    }'
```

Lorsque vous omettez`versionId`, Lambda utilise la dernière version de l'objet au moment de sa création.

Pour créer une nouvelle révision avec une version d'objet spécifique (AWS CLI)

- Exécutez la commande suivante pour créer une nouvelle révision qui utilise une version spécifique de votre package de déploiement.

```
aws lambda-web create-web-function-revision \
    --function-name my-web-app \
    --build-config '{
      "codeConfig": {
        "s3Object": {
          "bucket": "my-bucket",
          "key": "my-app.zip",
          "versionId": "abc123def456"
        }
```

```
    },
    "runtimeConfig": { "runtime": "nodejs24.x" }
}' \
--service-config '{
    "executionRoleArn": "arn:aws:iam::111122223333:role/my-web-function-role"
}'
```

En spécifiant`versionId`, vous épinglez la révision sur une version exacte de l'objet plutôt que sur la dernière version.

Cycle de vie des objets

> **Ne supprimez pas les objets S3 et ne supprimez pas l'accès Lambda pour les révisions actives**
>
> Lambda référence votre code depuis votre compartiment Amazon S3. Si vous supprimez l'objet S3 utilisé par une révision, ou la version d'objet spécifique utilisée par la révision, la révision passe à l'`Failed`état lorsque Lambda vérifie ensuite l'accès à l'objet, puis ne peut plus desservir le trafic. Conservez les versions des objets pour toutes les révisions que vous utilisez encore.
> La suppression de l'accès du principal du service Lambda au bucket a le même effet. Si vous modifiez la politique de compartiment pour refuser ou supprimer `s3:GetObject` et `s3:GetObjectVersion` les autorisations pour`lambda.amazonaws.com`, les révisions existantes qui font référence aux objets de ce compartiment passent à l'`Failed`état. Conservez à la fois les objets et l'accès en lecture du principal du service Lambda tant qu'une révision fait référence à ces objets.
> L'`Failed`État est permanent. La restauration de l'objet supprimé ou des autorisations du bucket ne renvoie pas de révision à l'`Active`état. Pour effectuer une restauration, créez une nouvelle révision qui fait référence à une version d'objet disponible, puis mettez à jour les poids de révision de vos points de terminaison pour acheminer le trafic vers cette version.
> Pour les modèles de déploiement, voirthe section called “Modèles de déploiement”.

Lambda ne détourne pas automatiquement le trafic d'une `Failed` révision. Les demandes acheminées par un point de terminaison vers une `Failed` révision sont rejetées avec le code d'état HTTP 409 et un en-tête de `lambda-web-error-type` réponse de`Platform.RevisionNotActive`. Si le point de terminaison pondère le trafic entre plusieurs

révisions, seule la part des demandes acheminées vers la `Failed` révision est affectée ; les demandes acheminées vers des révisions saines sont traitées normalement. Pour mettre fin aux échecs, mettez à jour les pondérations de révision du point de terminaison afin de supprimer la `Failed` révision.

Le remplacement de l'objet par un nouveau téléchargement crée une nouvelle version de S3. Cela n'affecte pas les révisions existantes : lorsque vous créez une révision, Lambda résout et épingle la version exacte de l'objet, même si vous l'omettez. `versionId` Toutefois, si vous supprimez une ancienne version d'objet à laquelle une révision fait référence, cette révision passe à l'`Failed`état actuel. Le téléchargement d'un objet de remplacement n'est pas utile, car le remplacement est une nouvelle version avec un ID de version différent.

Multi-Region déploiements

Pour les fonctions Web avec `MultiRegion` ou `PerRegion` points de terminaison, Lambda lit votre objet source à partir du compartiment que vous spécifiez, quelle que soit la région dans laquelle se trouve le compartiment. Lambda réplique ensuite l'artefact de code préparé qu'il dérive de cet objet vers les autres régions. Il n'est pas nécessaire de copier votre package de déploiement dans des compartiments situés dans d'autres régions. Pour plus d'informations sur ce que Lambda réplique, consultez. the section called “Ce que Lambda reproduit”

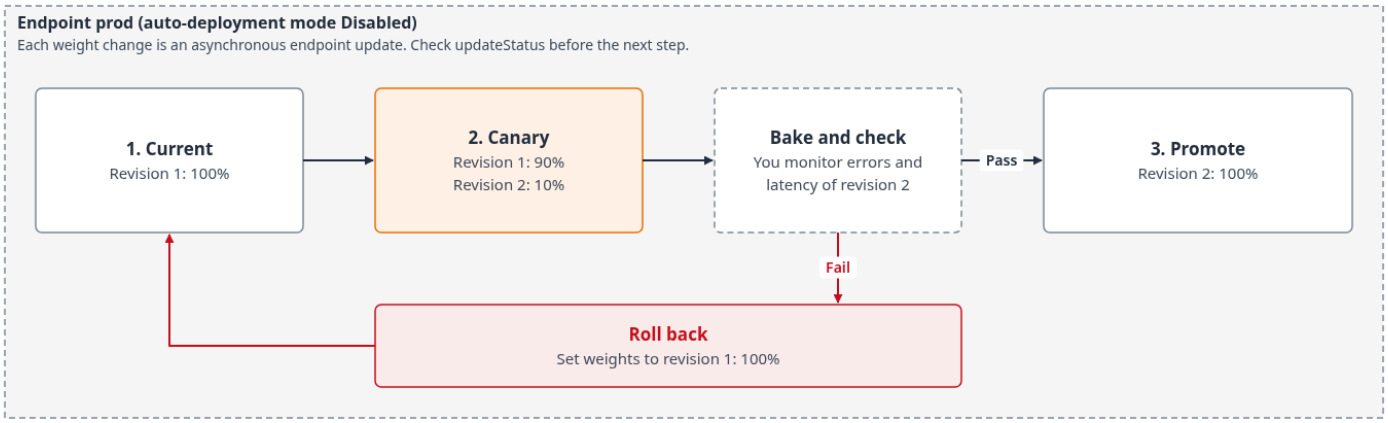
Modèles de déploiement

Pour publier une nouvelle version de votre application AWS Lambda Web Function, vous devez créer une nouvelle révision. Les points de terminaison sont `autoDeploymentMode` configurés pour LatestRevisionacheminer tout le trafic vers celui-ci une fois qu'il est devenu actif. Les points de terminaison `autoDeploymentMode` définis sur Désactivé continuent de diffuser leurs révisions actuelles jusqu'à ce que vous mettiez à jour les pondérations de révision. Vous contrôlez la manière dont le trafic passe de la révision actuelle à la nouvelle à l'aide du mode de déploiement automatique du terminal et des pondérations de révision. Les sections suivantes expliquent à la fois les modes de déploiement automatique, les modèles de déploiement courants (canari, bleu-vert et rollback) et les règles qui régissent les pondérations de révision.

Les modifications apportées aux points `autoDeploymentMode` de terminaison `revisionWeights` sont des mises à jour asynchrones. Attendez `updateStatus` de devenir `Successful` avant d'évaluer le déploiement ou de soumettre une autre mise à jour du terminal. En cas d'échec d'une mise à jour, `updateStatusReason` décrit la cause.

Le schéma suivant montre un déploiement Canary sur un terminal dont le mode de déploiement automatique est désactivé. Chaque modification de poids est une mise à jour asynchrone du point de terminaison.

1. La révision 1 commence avec 100 % du trafic.
2. Vous acheminez 10 % du trafic vers la révision 2 et vous le surveillez.
3. Si la révision 2 passe avec succès vos vérifications, vous acheminez tout le trafic vers elle.
4. Si la révision 2 échoue, vous redéfinissez les pondérations sur la révision 1 à 100 %.



Rolling back is another endpoint update, not an instant switch. Keep the earlier revision until the new one is stable.

Auto-deployment modes

Le `autoDeploymentMode` paramètre d'un point de terminaison contrôle si Lambda achemine automatiquement le trafic vers les nouvelles révisions lors du déploiement. Vous le définissez lorsque vous créez le point de terminaison, et vous pouvez le modifier sur un point de terminaison existant.

Si vous omettez`autoDeploymentMode`, la valeur par défaut est. `Disabled` `LatestRevision`n'est pris en charge que pour les `HomeRegion` points de terminaison, donc `MultiRegion` et les `PerRegion` points de terminaison l'utilisent toujours. `Disabled` Lors de l'utilisation`Disabled`, vous le définissez `revisionWeights` sur le point de terminaison, comme décrit dansthe section called “Pondérations de révision”.

LatestRevision

> Chaque fois qu'une nouvelle révision devient active, Lambda achemine 100 % du trafic du point de terminaison vers celle-ci. Vous n'avez pas besoin de mettre à jour les pondérations de révision et vous ne pouvez pas définir de pondérations de révision lorsque le point final est dans ce mode.

Utilisez ce mode pour les environnements de développement et de préparation dans lesquels vous souhaitez un déploiement automatique sans intervention manuelle.

Désactivé

Lambda ne modifie pas le routage du trafic lorsque vous créez une nouvelle révision. Vous contrôlez le routage du trafic manuellement en définissant des pondérations de révision. Utilisez ce mode pour les environnements de production dans lesquels vous souhaitez contrôler le déploiement de nouvelles révisions à l'aide de modèles de déploiement Canary ou Blue-Green.

Pour modifier le mode de déploiement automatique (AWS CLI)

1. Utilisez le AWS Command Line Interface (AWS CLI) pour mettre à jour le point de terminaison et désactiver le déploiement automatique.

```
aws lambda-web update-web-function-endpoint \
    --function-name my-web-app \
    --endpoint-name my-endpoint \
    --auto-deployment-mode Disabled
```

2. Attendez que la mise à jour du terminal soit terminée.

```
aws lambda-web wait web-function-endpoint-updated \
    --function-name my-web-app \
    --endpoint-name my-endpoint
```

Basculement entre les modes

Lorsque vous passez de Disabled LatestRevisionà Disabled sans spécifier de pondération de révision, le routage actuel du trafic reste inchangé une fois la mise à jour réussie. La révision vers laquelle le terminal acheminait le trafic avant la mise à jour continue de recevoir 100 % du trafic, même après que vous ayez créé de nouvelles révisions. Il conserve ce trafic jusqu'à ce que vous mettiez à jour les pondérations de révision. Vous pouvez également changer de mode et définir les poids de révision dans la même `UpdateWebFunctionEndpoint` demande.

Lorsque vous passez de Disabled à LatestRevision, Lambda met à jour le point de terminaison pour acheminer 100 % du trafic vers la dernière révision. La dernière révision doit être active. Si elle est en attente ou en échec, la demande échoue avec une erreur de conflit. Une fois la mise à jour réussie, les pondérations de révision précédemment configurées ne s'appliquent plus.

Pondérations de révision

Lorsque le mode de déploiement automatique est désactivé, vous contrôlez le routage du trafic en attribuant des pondérations aux révisions. Lambda répartit le trafic entre les révisions proportionnellement à leur pondération.

Les pondérations de révision sont un paramètre du point de terminaison (la `revisionWeights` propriété), que vous pouvez modifier`UpdateWebFunctionEndpoint`. Ils ne constituent pas un paramètre de révision.

Les pondérations de révision suivent les règles suivantes :

- Chaque poids est un entier compris entre 1 et 100.
- La somme des poids d'une demande doit être exactement égale à 100.
- Chaque révision ne peut apparaître qu'une seule fois dans les pondérations.
- Chaque révision des pondérations doit être à l'état Actif lorsque vous définissez les pondérations. Dans le cas contraire, l'API rejette la demande.
- Un point de terminaison achemine le trafic vers un maximum de deux révisions en même temps.
- Aucun poids n'a de valeur par défaut. Pour acheminer tout le trafic vers une seule révision, spécifiez uniquement cette révision avec une pondération de 100. Une révision qui ne figure pas dans les pondérations ne reçoit aucun trafic en provenance de ce point de terminaison.

Les identifiants de révision sont générés par Lambda lorsque vous créez une révision. Pour trouver les identifiants de révision de votre fonction Web, utilisez la commande suivante :

```
aws lambda-web list-web-function-revisions \
    --function-name my-web-app
```

La réponse répertorie les révisions du plus récent au plus ancien, y compris leurs identifiants, leurs horodatages de création et leur état actuel.

Modèles de déploiement

Les modèles de déploiement suivants utilisent des pondérations de révision pour contrôler le transfert du trafic entre votre révision actuelle et une nouvelle révision. Ces modèles nécessitent que le mode de déploiement automatique du point de terminaison (le paramètre du point de

`autoDeploymentMode` terminaison) soit désactivé. Le point de terminaison créé par la `aws lambda-web deploy` commande utilise LatestRevision. Pour utiliser ces modèles sur ce point de terminaison, basculez-le d'abord sur Disabled, comme indiqué dansthe section called “Auto-deployment modes”.

Déploiement Canary

Un déploiement de Canary envoie un faible pourcentage du trafic vers la nouvelle révision afin que vous puissiez détecter les erreurs avant d'acheminer tout le trafic. Si la nouvelle révision présente des problèmes, seule une petite partie des demandes est affectée.

Pour effectuer un déploiement Canary (AWS CLI)

1. Créez une nouvelle révision avec votre code mis à jour.

```
aws lambda-web create-web-function-revision \
    --function-name my-web-app \
    --build-config '{
      "codeConfig": {
        "s3Object": { "bucket": "my-bucket", "key": "my-app-v2.zip" }
      },
      "runtimeConfig": { "runtime": "nodejs24.x" }
    }' \
    --service-config '{
      "executionRoleArn": "arn:aws:iam::111122223333:role/my-web-function-role"
    }'
```

   Notez l'identifiant de révision dans la réponse.

   Une nouvelle révision ne copie pas les paramètres de la révision actuelle. Tout `serviceConfig` paramètre que vous omettez prend sa valeur par défaut, par exemple 30 et aucune variable `timeoutSeconds` d'environnement. Incluez tous les paramètres utilisés par la révision en cours`environmentVariables`, tels que`timeoutSeconds`,`maxConcurrencyPerEnvironment`, et`telemetryConfig`. Pour voir la configuration de la révision actuelle, exécutez`aws lambda-web get-web-function-revision`.

2. Patientez jusqu'à ce que la nouvelle révision soit active. L'API rejette les pondérations de révision qui font référence à une révision qui n'est pas active.

```
aws lambda-web wait web-function-revision-active \
```

```
    --function-name my-web-app \
    --revision-id rev-def45
```

3. Acheminez 10 % du trafic vers la nouvelle révision et 90 % vers la révision actuelle.

```
aws lambda-web update-web-function-endpoint \
    --function-name my-web-app \
    --endpoint-name my-endpoint \
    --revision-weights '[{"revisionId": "rev-abc12", "weight": 90}, {"revisionId":
 "rev-def45", "weight": 10}]'
```

4. Attendez que la mise à jour du terminal soit terminée.

```
aws lambda-web wait web-function-endpoint-updated \
    --function-name my-web-app \
    --endpoint-name my-endpoint
```

5. Surveillez la nouvelle révision via les journaux des applications ou des métriques personnalisées. Incluez-y un identifiant de construction ou de révision que vous contrôlez. Les métriques des fonctions Web n'incluent pas de dimension de révision. Par conséquent, ils ne peuvent pas séparer les erreurs Canary des erreurs de la révision en cours. Pour plus de détails, consultez the section called “Métriques”. Si le canari atteint les seuils d'erreur et de latence que vous avez définis avant le déploiement, augmentez son poids.

```
aws lambda-web update-web-function-endpoint \
    --function-name my-web-app \
    --endpoint-name my-endpoint \
    --revision-weights '[{"revisionId": "rev-abc12", "weight": 50}, {"revisionId":
 "rev-def45", "weight": 50}]'
```

6. Attendez que la mise à jour du terminal soit terminée.

```
aws lambda-web wait web-function-endpoint-updated \
    --function-name my-web-app \
    --endpoint-name my-endpoint
```

7. Lorsque vous êtes certain que la nouvelle révision est saine, acheminez tout le trafic vers celle-ci.

```
aws lambda-web update-web-function-endpoint \
    --function-name my-web-app \
    --endpoint-name my-endpoint \
```

```
    --revision-weights '[{"revisionId": "rev-def45", "weight": 100}]'
```

8. Attendez que la mise à jour du terminal soit terminée.

```
aws lambda-web wait web-function-endpoint-updated \
    --function-name my-web-app \
    --endpoint-name my-endpoint
```

Blue-green déploiement

Un déploiement bleu-vert conserve le trafic de la révision actuelle pendant que vous validez la nouvelle révision, puis fait passer tout le trafic vers la nouvelle révision dans une seule mise à jour du point de terminaison. La procédure suivante permet de valider avec une répartition uniforme du trafic. Pour valider sans trafic de production, utilisez un point de terminaison de test distinct, comme décrit dansthe section called “Considérations relatives au déploiement”.

Pour effectuer un déploiement bleu-vert (AWS CLI)

1. Créez une nouvelle révision avec votre code mis à jour et attendez qu'elle soit active. Utilisez les mêmes commandes que celles indiquées dans la procédure de déploiement de Canary précédente.
2. Répartissez le trafic de manière égale entre les deux révisions.

```
aws lambda-web update-web-function-endpoint \
    --function-name my-web-app \
    --endpoint-name my-endpoint \
    --revision-weights '[{"revisionId": "rev-abc12", "weight": 50}, {"revisionId":
 "rev-def45", "weight": 50}]'
```

3. Attendez que la mise à jour du terminal soit terminée.

```
aws lambda-web wait web-function-endpoint-updated \
    --function-name my-web-app \
    --endpoint-name my-endpoint
```

4. Surveillez les deux révisions via les journaux des applications ou des métriques personnalisées. Incluez-y un identifiant de construction ou de révision que vous contrôlez. Lorsque la nouvelle révision répond aux critères d'intégrité que vous avez définis avant le déploiement, acheminez tout le trafic vers celle-ci.

```
aws lambda-web update-web-function-endpoint \
    --function-name my-web-app \
    --endpoint-name my-endpoint \
    --revision-weights '[{"revisionId": "rev-def45", "weight": 100}]'
```

5. Attendez que la mise à jour du terminal soit terminée.

```
aws lambda-web wait web-function-endpoint-updated \
    --function-name my-web-app \
    --endpoint-name my-endpoint
```

Faire marche arrière

Si vous détectez des problèmes liés à une nouvelle révision (taux d'erreur élevés, latence accrue), vous pouvez revenir en arrière avec une seule mise à jour du point de terminaison qui achemine tout le trafic vers la révision précédente, dont le fonctionnement a été vérifié.

> **Revenir en LatestRevision mode**
>
> Lorsque le mode de déploiement automatique d'un point de terminaison est activé LatestRevision, une demande qui définit uniquement les pondérations de révision échoue. La procédure suivante définit le mode de déploiement automatique sur Désactivé et les pondérations de révision dans la même demande, afin que cela fonctionne dans les deux modes.
>
> Le point de terminaison reste ensuite en mode désactivé jusqu'à ce que vous le modifiiez.

Pour revenir à une révision précédente (AWS CLI)

1. Mettez à jour le point de terminaison pour acheminer 100 % du trafic vers la version dont le fonctionnement a été vérifié et définissez le mode de déploiement automatique sur Disabled.

```
aws lambda-web update-web-function-endpoint \
    --function-name my-web-app \
    --endpoint-name my-endpoint \
    --auto-deployment-mode Disabled \
    --revision-weights '[{"revisionId": "rev-abc12", "weight": 100}]'
```

2. Attendez que la mise à jour du terminal soit terminée.

```
aws lambda-web wait web-function-endpoint-updated \
    --function-name my-web-app \
    --endpoint-name my-endpoint
```

Une fois la mise à jour réussie, Lambda arrête d'acheminer les nouvelles demandes vers la révision problématique. In-flight les demandes relatives à cette révision se terminent normalement. Pour plus d'informations sur l'état de mise à jour des terminaux, consultezthe section called “États de point de terminaison”.

Si la révision à laquelle vous revenez ne comporte que peu ou pas d'environnements d'exécution en cours d'exécution, Lambda la fait évoluer au fur et à mesure que le trafic s'y déplace. Les demandes peuvent attendre l'initialisation des environnements d'exécution, ce qui augmente le temps de latence. Les demandes peuvent toujours échouer en raison d'échecs de démarrage, de la limite de débit ou du nombre maximal d'environnements du point de terminaison, ou du quota de vCPU du compte. Certains de ces échecs renvoient des réponses HTTP 429.

Considérations relatives au déploiement

Qu'est-ce qui déclenche une nouvelle révision ?

Lambda crée une nouvelle révision lorsque vous appelez. `CreateWebFunctionRevision` Cela inclut le déploiement d'un nouveau code d'application et la modification des paramètres de configuration tels que le délai d'expiration, la simultanéité ou les variables d'environnement. Chaque modification produit une révision immuable.

Puis-je tester une nouvelle révision avant d'y acheminer le trafic de production ?

Oui. Vous ne pouvez appeler une révision que par le biais d'un point de terminaison. Il existe donc deux approches :

- Point de terminaison de test dédié : créez un point de terminaison distinct pour les tests. Acheminez d'abord le trafic vers la nouvelle révision sur le point de terminaison de test (en définissant les poids de révision du point de terminaison de test), validez-le, puis mettez à jour les poids du point de terminaison de production pour inclure la nouvelle révision.
- Poids minimal : attribuez à la nouvelle révision une pondération de 1 % sur le point final de production. Cela envoie une petite fraction du trafic de production vers la nouvelle révision afin que vous puissiez surveiller les erreurs avec un impact minimal sur le client.

Qu'arrive-t-il aux révisions qui ne sont pas incluses dans les pondérations de révision ?

Une révision qui ne figure pas dans les pondérations de révision d'un point de terminaison ne reçoit aucun trafic en provenance de ce point de terminaison. Un autre point de terminaison de la même fonction Web peut toujours y accéder. La révision reste active jusqu'à ce que vous la supprimiez ou jusqu'à ce qu'un nettoyage automatique la supprime. Il passe au statut Failed si Lambda perd l'accès à son objet Amazon S3. Pour le nettoyage automatique, voirthe section called “Limites de révision et nettoyage automatique”.

Comment puis-je identifier la révision la plus récente ?

Appelez `ListWebFunctionRevisions`. La réponse répertorie les révisions par ordre décroissant de`createdAt`, de sorte que la première révision de la liste est la plus récente.

Puis-je supprimer un point de terminaison pendant qu'il achemine du trafic ?

Oui. Lorsque vous supprimez un point de terminaison, Lambda arrête d'acheminer les nouvelles demandes vers ce point de terminaison et les demandes adressées au nom de domaine du point de terminaison sont rejetées une fois que la suppression prend effet. Les révisions elles-mêmes ne sont pas affectées et peuvent toujours être utilisées par d'autres points de terminaison.

Puis-je supprimer une révision alors qu'elle reçoit du trafic ?

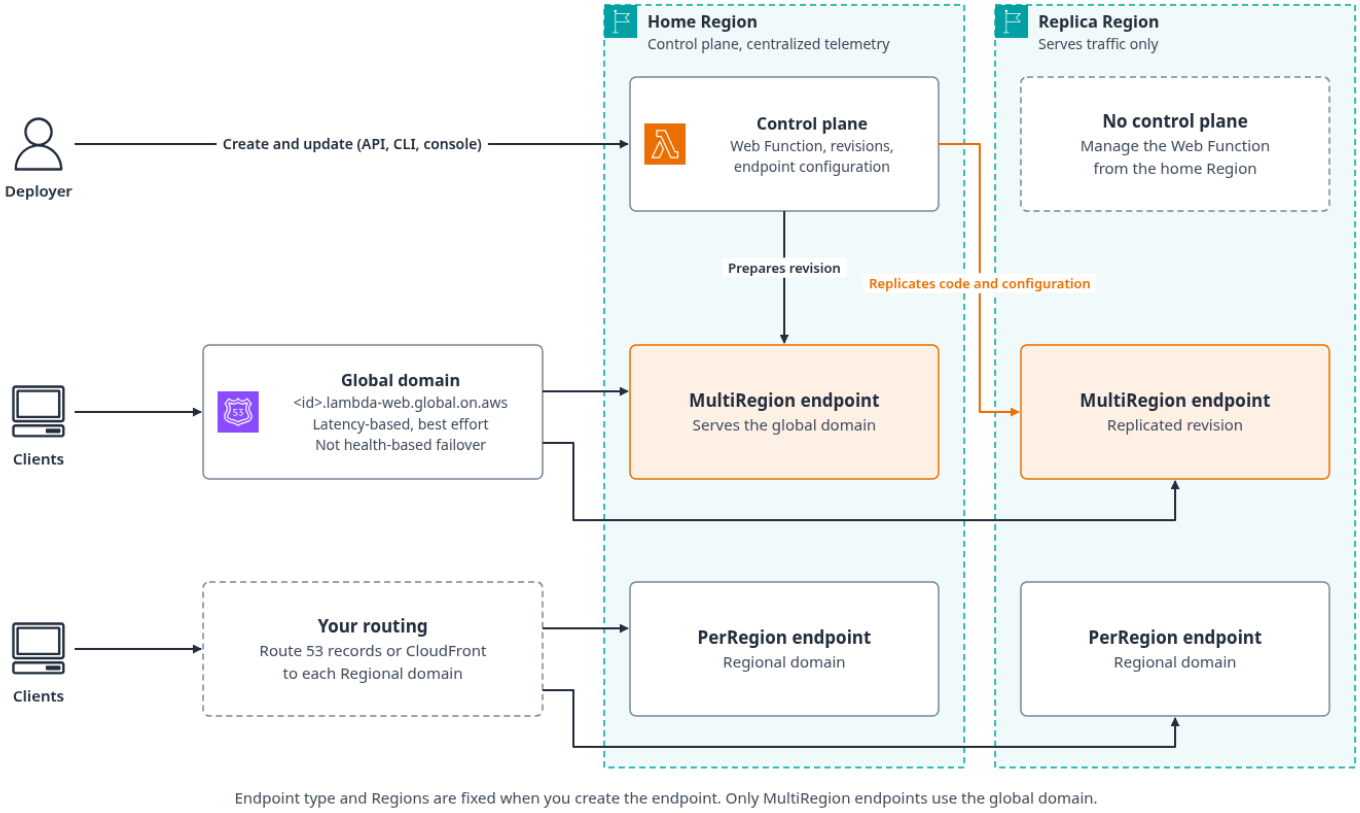
Non Si un point de terminaison achemine le trafic vers la révision, y compris lorsque la `regionalEndpoints` propriété d'un point de `PerRegion` terminaison `MultiRegion` ou d'un point de terminaison fait référence à la révision, la `DeleteWebFunctionRevision` demande échoue avec une erreur de conflit. Pour supprimer la révision, mettez d'abord à jour les poids de révision du point de terminaison afin de le supprimer du routage du trafic sur chaque point de terminaison, puis supprimez-le. Comme Lambda bloque la suppression alors qu'une pondération est attribuée à une révision, la suppression d'une révision ne modifie jamais la distribution du trafic d'un point de terminaison.

Multi-Region déploiement

Pour les points de PerRegionterminaison MultiRegionet les points de terminaison, Lambda réplique les artefacts d'exécution dans toutes les régions cibles afin que votre application puisse desservir le trafic à proximité des utilisateurs finaux. Vous gérez la fonction Web entièrement depuis la région d'origine. Les ressources répliquées ne sont ni visibles ni modifiables dans les régions de réplication.

Le schéma suivant montre comment le plan de contrôle de la région d'origine prépare une révision et réplique son code et sa configuration dans une région de réplication, et comment les clients

atteignent MultiRegionles points de PerRegionterminaison. Une région de réplique ne possède aucun plan de contrôle. Un MultiRegionpoint de terminaison possède un domaine global qui est acheminé par latence, et non par état de santé de la région. Pour un PerRegionpoint de terminaison, vous gérez la manière dont les clients accèdent au domaine régional dans chaque région, par exemple avec les enregistrements Route 53 ou CloudFront. Vous définissez le type de point de terminaison et les régions lorsque vous créez le point de terminaison, et vous ne pourrez pas les modifier ultérieurement.



Rubriques

- Ce que Lambda reproduit
- Visibilité des répliques
- Quand la réplication a lieu
- Fonctionnement du routage
- Défaillances de réplication
- Cohérence à terme

Ce que Lambda reproduit

Lambda réplique les éléments suivants dans chaque région cible :

- Artefact de code préparé : artefact d'exécution interne que Lambda dérive de l'objet source Amazon S3 versionné.
- Configuration des révisions : délai d'expiration, simultanéité, variables d'environnement et paramètres d'exécution.
- Resource-based politiques — Politiques associées à la fonction Web qui accordent l'accès à celle-ci.
- Balises — Les balises de la fonction Web.

Les quotas pour les fonctions Web s'appliquent par Région AWS. Chaque région cible applique ses propres quotas de compte sur le point de terminaison répliqué. Par exemple, le dimensionnement de l'environnement d'exécution dans une région de réplication est limité par le quota de vCPU du compte de cette région. Pour les quotas de compte, voirthe section called “Quotas de comptes”.

Visibilité des répliques

Les ressources répliquées ne sont pas visibles dans les régions de réplication. Le plan de contrôle d'une fonction Web n'est desservi que dans sa région d'origine, de sorte que toutes les demandes d'API doivent être envoyées à la région d'origine. Cela inclut notamment les éléments suivants :

- Répertoriez, obtenez et décrivez les demandes relatives à la fonction Web, à ses révisions et à ses points de terminaison.
- Créez, mettez à jour et supprimez des demandes pour la fonction, les révisions et la configuration du point de terminaison.

Une demande d'API envoyée au point de terminaison du plan de contrôle d'une région répliquée échoue, quel que soit l'endroit où se trouve l'appelant. Les artefacts d'exécution répliqués existent uniquement pour que le plan de données serve le trafic.

Quand la réplication a lieu

La réplication est déclenchée lorsque vous créez ou mettez à jour un MultiRegionpoint de PerRegionterminaison. Plus précisément, la réplication a lieu lorsque :

- Vous créez un point de PerRegion terminaison MultiRegion ou avec des pondérations de révision pointant vers une révision.
- Vous mettez à jour les pondérations de révision sur un MultiRegion PerRegion point de terminaison pour inclure une nouvelle révision.
- Vous mettez à jour d'autres paramètres de point de terminaison`authType`, tels que`scalingConfig`, ou`throttleConfig`, sur un point de PerRegion terminaison MultiRegion ou.

La création d'une révision à elle seule ne déclenche pas la réplication. La révision doit être incluse dans les poids de révision d'un point de terminaison dont les régions cibles sont configurées. Étant donné que seul le mode de déploiement automatique désactivé est disponible pour les PerRegion terminaux MultiRegion et les terminaux, la réplication est toujours le résultat d'une modification apportée au point de terminaison.

Fonctionnement du routage

Le comportement du routage dépend du type de point de terminaison :

MultiRegion

Lambda fournit un nom de domaine global unique. Les demandes sont acheminées à l'aide d'un routage basé sur la latence. Les demandes sont acheminées vers la région qui fournit généralement la latence réseau la plus faible pour l'appelant, sur la base des mesures de latence collectées par Route 53 au fil du temps. Étant donné que la latence d'Internet change, Lambda ne garantit pas que chaque requête soit envoyée vers la région à latence la plus faible. Lambda gère automatiquement les itinéraires pour vous.

PerRegion

Lambda fournit un nom de domaine régional distinct dans chaque région cible. Vous êtes responsable de la gestion de la manière dont le trafic atteint chaque domaine régional. Par exemple, vous pouvez configurer votre propre politique de routage Route 53 ou placer une CloudFront distribution devant les domaines régionaux.

Défaillances de réplication

La réplication peut échouer dans une région en raison d'un problème de service temporaire. Si vous chiffrez votre fonction Web avec une clé gérée par le client, une réplique de clé manquante dans la

région cible entraîne également l'échec de la réplication. Pour les principales exigences relatives à plusieurs régions, voirthe section called “Configuration d'une clé gérée par le client”.

L'effet d'un échec de réplication dépend de la création ou de la mise à jour du point de terminaison. Si la réplication échoue dans une région pendant que Lambda crée le point de terminaison, le point de terminaison passe à l'état d'échec et n'est invoquable dans aucune région. Pour réessayer, supprimez le point de terminaison et créez-le à nouveau. Si la réplication échoue dans une région lors de la mise à jour d'un terminal, l'échec est limité à cette région. Le point de terminaison reste invocable et les autres régions continuent de fonctionner normalement.

Lorsque la réplication d'une nouvelle révision échoue dans une région, cette région continue de desservir le trafic en utilisant la révision précédente qui a été déployée avec succès. Le point de terminaison ne revient pas en arrière. Il continue de fonctionner avec le dernier bon état connu de chaque région.

Vous pouvez consulter l'état de chaque région et le mettre à jour dans le `regionalEndpoints` champ de la `GetWebFunctionEndpoint` réponse. L'inscription de chaque région inclut :

- `state`et `stateReason` — État de déploiement de la région lors de la création du point de terminaison.
- `updateStatus`et `updateStatusReason` — Le résultat de la dernière mise à jour (par exemple, le déploiement d'une révision) pour cette région.

Pour résoudre un échec de réplication, traitez la cause première (par exemple, créez une réplique AWS KMS clé dans la région affectée). Pour réessayer la mise à jour d'un terminal qui a échoué une fois que vous en avez résolu la cause première, appelez `UpdateWebFunctionEndpoint` à nouveau. Vous pouvez répéter les mêmes paramètres ou spécifier uniquement le nom de la fonction et le nom du point de terminaison. L'une ou l'autre demande lance un nouveau déploiement dans les régions cibles. Cela ne fonctionne que lorsque le point de terminaison est actif. Si la création du point de terminaison a échoué, supprimez-le et créez-le à nouveau.

Cohérence à terme

La réplication des artefacts d'exécution est finalement cohérente. Ne partez pas du principe que chaque région exécute la nouvelle configuration tant que chaque région ne figure pas `updateStatus` dans `regionalEndpoints` les rapports`Successful`.

Resource-based les modifications de politique peuvent cesser de se propager après les modifications du code et de la configuration. Au cours de la fenêtre de réplication, les demandes dans les régions

de réplication peuvent être évaluées par rapport à la version précédente de la politique. Pour plus d'informations, consultez the section called “Réplication et cohérence éventuelle”.

Requêtes et réponses HTTP

Un point de terminaison Web Function accepte les HTTP/1.1 demandes et les transmet à votre application HTTP/1.1. Lambda rejette les HTTP/1.0 requêtes via HTTP 505 (version HTTP non prise en charge). Lambda préserve la méthode de requête, le chemin, la chaîne de requête, le corps et la plupart des en-têtes. Il supprime ou modifie les en-têtes qui décrivent la connexion entre le client et le point de terminaison. Il ajoute également des en-têtes qui fournissent le contexte de la demande.

Méthodes HTTP

Les points de terminaison Web Function prennent en charge `GET` `HEADPOST`,`PUT`,`PATCH`,`OPTIONS`, et`DELETE`.

Lambda rejette une méthode non prise en charge avec une réponse HTTP 400 avant que la demande n'atteigne votre application.

En-têtes de demandes

Lambda supprime les en-têtes suivants avant de transmettre une demande :

- `Connection`, `Keep-Alive`, `Upgrade`, `Expect`, `TE`, et `Trailer`
- `Proxy-Authenticate`, `Proxy-Authorization` et `Proxy-Connection`
- `X-Real-IP`
- `X-HTTP-Method-Override`, `X-HTTP-Method` et `X-Method-Override`
- En-têtes dont le nom commence `lambda-web-` par et en-têtes nommés dans l'en-tête `Connection`

Lambda valide ou modifie les en-têtes suivants.

En-tête	Comportement
`Host`	Doit être le nom de domaine du point de terminaison de la fonction Web (par exemple,`bcdfghjklmnpqrst.b7t.lambda-web.us-east-1.on.aws`), en minuscules et sans port. Lambda achemine sur cette valeur et renvoie HTTP 404 si elle ne correspond pas à un point de

En-tête	Comportement
	terminaison, ou HTTP 400 si l'en-tête est manquant. Votre application reçoit le nom de domaine du point de terminaison.
`X-Forwarded-For`	Lambda ajoute l'adresse IP du client qui se connecte comme dernière valeur. Les valeurs antérieures proviennent du client et ne sont pas validées. Lorsqu'une CloudFront distribution Amazon se trouve devant le point de terminaison, la dernière valeur est une CloudFront adresse.

Lambda effectue des transferts `X-Forwarded-Host` depuis le client sans validation. Ne l'utilisez pas pour créer des redirections, des URL absolues ou des autorisations basées sur l'hôte, sauf si une porte d'entrée que vous contrôlez le définit.

Lambda ajoute les en-têtes suivants.

En-tête	Description
`lambda-web-request-id`	Identifiant que Lambda attribue à la demande.
`lambda-web-endpoint-name`	Le nom du point de terminaison qui a reçu la demande.

Pour les points de terminaison qui utilisent l'autorisation IAM, Lambda valide la demande signée et supprime l'en-tête avant de la `Authorization` transmettre. Pour plus d'informations, consultez the section called “Utilisation du type `IamAuth`d'authentification”.

En-têtes de réponse

Lambda supprime les en-têtes et les bandes-annonces HTTP limités à la connexion de la réponse de votre application. En fonction du résultat de la demande, Lambda peut ajouter les en-têtes suivants.

En-tête	Description
`lambda-web-request-id`	L'identifiant de la demande. Utilisez-le pour corréler une réponse avec les journaux de l'application et du système.

En-tête	Description
`lambda-web-logstream`	Le flux de journal Amazon CloudWatch Logs qui contient les journaux de l'environnement d'exécution qui a traité la demande.
`lambda-web-error-type`	Type d'erreur, au format `<Prefix>.<ErrorReason>` (par exemple, `Platform.EndpointRequestThrottle` ou`Runtime.RequestTimeout`). Lambda omet cet en-tête pour les erreurs de service internes et les échecs d'autorisation. Pour la liste des valeurs, voirthe section called “Types d'erreur liés aux fonctions Web”.

Limites d'en-têtes

La ligne de demande, les en-têtes de demande et la ligne vide finale peuvent totaliser jusqu'à 128 KiB. Lambda rejette une demande qui dépasse cette limite avec le protocole HTTP 431 (champs d'en-tête de demande trop grands) avant que la demande n'atteigne votre application. Pour le dépannage, voirthe section called “Limites des en-têtes de demande”.

Configuration de la mise en réseau pour AWS Lambda Fonctions Web

Une fonction Web accepte les demandes des clients. Il peut également accéder à d'autres ressources pour effectuer son travail, comme une base de données dans votre VPC, une API interne ou un service sur Internet public. Vous configurez ces deux directions indépendamment. Vous pouvez exposer un point de terminaison aux appelants sans lui accorder un accès VPC, ou accorder à une fonction un accès sortant privé sans changer qui peut l'invoquer.

Le trafic entrant atteint une fonction Web via un point de terminaison. Le point de terminaison définit son nom de domaine, son type de point de terminaison, ses régions et sa configuration d'autorisation. Le trafic sortant est configuré lors d'une révision. Une révision sans connecteur réseau de sortie atteint directement les `IPv4` destinations publiques. Une révision qui fait référence à un connecteur envoie son trafic sortant via votre VPC. Une fonction Web s'exécute sur une infrastructure que Lambda possède et gère, et non au sein de votre VPC. Un connecteur réseau de sortie ajoute uniquement un accès VPC sortant. Cela ne change pas la manière dont les clients atteignent le point de terminaison ni les personnes autorisées à l'invoquer.

> **Note**
>
> Les noms de domaine des points de terminaison Web Function sont accessibles depuis l'Internet public. AWS PrivateLink les points de terminaison d'interface ne sont pas disponibles pour les noms de domaine de point de terminaison des fonctions Web. Utilisez la configuration d'autorisation du terminal pour contrôler l'accès.

Connectivité entrante

Les clients invoquent une fonction Web via un point de terminaison HTTPS Lambda-managed public. Lambda met fin au protocole TLS et transmet la demande au serveur HTTP de votre application. Le point de terminaison géré prend en charge HTTP/1.1. Il n'expose pas d'adresse VPC privée et n'accepte pas de connexions directes à l'environnement d'exécution.

`IamAuth`contrôle qui peut invoquer un point de terminaison, mais cela ne rend pas le point de terminaison privé au niveau de la couche réseau. Pour les options d'autorisation, voirthe section called “Contrôle d’accès”.

Le point de terminaison contrôle le routage, l'autorisation, la régulation et le dimensionnement des demandes. Son type de point de terminaison et son ensemble de régions sont fixes lorsque vous le créez. Pour modifier l'une ou l'autre des propriétés, créez un nouveau point de terminaison et déplacez les clients vers son nouveau nom de domaine.

La configuration du point de terminaison est indépendante de la sortie du VPC. L'ajout d'un connecteur réseau de sortie à une révision ne rend pas le point de terminaison privé et ne limite pas les demandes entrantes.

> **Important**
>
> Vous ne pouvez utiliser les connecteurs réseau de sortie qu'avec des points de `HomeRegion` terminaison. Lambda rejette les tentatives de routage d'un `MultiRegion` point de `PerRegion` terminaison vers une révision qui fait référence à un connecteur réseau de sortie.

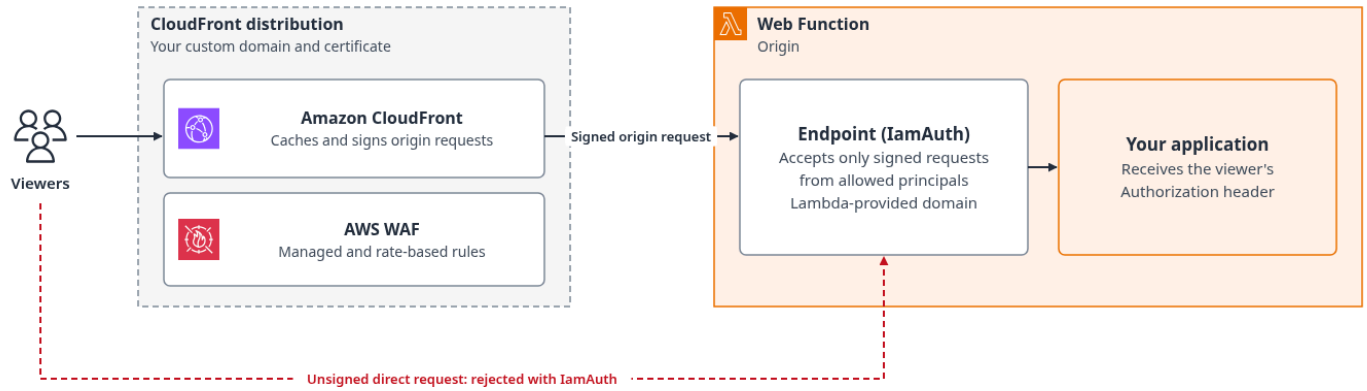
Lorsque les pondérations de révision répartissent le trafic entre des révisions avec des configurations de connecteurs différentes, les demandes utilisent des chemins réseau différents. Lorsque vous

diagnostiquez une connectivité intermittente, vérifiez d'abord le mode de déploiement automatique du terminal et les pondérations de révision. Pour savoir comment ils acheminent les demandes vers les révisions, voirthe section called “Modèles de déploiement”.

Ajouter une porte d'entrée HTTP devant un point de terminaison

Une porte d'entrée est un service qui reçoit les demandes des clients et les transmet à votre terminal. Il ajoute des fonctionnalités telles qu'un domaine personnalisé, la mise en cache ou la protection par pare-feu des applications Web. Les points de terminaison Web Function ne prennent pas en charge les noms de domaine personnalisés ni AWS WAF l'association directe. Utilisez Amazon CloudFront devant le point de terminaison lorsque vous avez besoin d'un domaine personnalisé, d'une mise en cache périphérique, HTTP/2 ou HTTP/3 entre le lecteur et le périphérique, d'une compression des réponses ou de AWS WAF contrôles.

Le schéma suivant montre une porte d'entrée de production. Un client se connecte à un domaine CloudFront personnalisé protégé par AWS WAF. CloudFront envoie la demande à un point de terminaison de fonction Web protégé, qui l'achemine vers un environnement d'exécution. Sans connecteur réseau de sortie, l'application peut appeler le AWS service public ou des points de terminaison Internet. Il ne peut pas accéder aux ressources qui n'ont que des adresses VPC privées. Pour accéder à ces ressources, voirthe section called “Connexion d'une fonction Web à votre VPC”. Avec`IamAuth`, CloudFront signe chaque demande d'origine et Lambda autorise la demande avant d'appeler votre fonction. Lambda préserve l'`Authorization`en-tête original du visualiseur et le transmet à votre fonction. Le Lambda-provided domaine accepte uniquement les demandes signées émanant des principaux autorisés à l'invoquer, et rejette les demandes directes non signées, telles qu'un navigateur appelant directement le domaine. Pour vous assurer que le point de terminaison accepte uniquement les appels provenant de votre distribution, ajoutez une politique basée sur les ressources qui accorde l'autorisation d'appel au principal du CloudFront service et l'étend au nom de ressource Amazon (ARN) de votre distribution avec une condition d'ARN source. Avec`ApplicationManaged`, le point de terminaison est public et les demandes directes contournent CloudFront et AWS WAF.



1. Configurez le domaine Web Function en tant qu'origine personnalisée HTTPS.
2. Joignez le certificat et le nom de domaine alternatif à la distribution, et faites pointer les enregistrements de votre système de noms de domaine (DNS) vers la distribution.
3. Transférez uniquement les en-têtes, les cookies et les chaînes de requête dont l'application a besoin. Ne transférez pas l'`Host`en-tête du visualiseur, car Lambda achemine `Host` et renvoie HTTP 404 lorsqu'il ne s'agit pas du domaine du point de terminaison. Si vous utilisez une politique de demande d'origine gérée qui transmet tous les en-têtes des lecteurs, choisissez`AllViewerExceptHostHeader`. Les limites d'en-têtes de point de terminaison incluent les en-têtes transférés.
4. (Facultatif) Joignez une ACL AWS WAF Web lorsque vous avez besoin d'une inspection par IP, par bot, basée sur le taux ou par règles gérées.
5. Protégez l'origine afin que les clients ne puissent pas contourner la distribution. Pour un IAM-authorized point de terminaison, accordez l'accès uniquement à l'identité d'entrée prévue. Pour une autorisation gérée par l'application, exigez et validez un secret d'origine ou une autre preuve au niveau de l'application attestant que la demande est bien passée par la distribution.

Pour la procédure CloudFront d'autorisation, voirthe section called “CloudFront intégration”.

Accès au navigateur et CORS

Lambda n'ajoute pas d'en-têtes CORS (Cross-Origin Resource Sharing) pour les fonctions Web. Votre demande ou votre porte d'entrée doit traiter les demandes avant le vol et les demandes réelles.

- Renvoie l'origine autorisée au lieu de refléter chaque `Origin` valeur.
- N'autorisez que les méthodes et les en-têtes de requête utilisés par l'application.

- Lorsque les navigateurs envoient des informations d'identification, utilisez une origine explicite et retournez`Access-Control-Allow-Credentials: true`. Ne combinez pas les informations d'identification avec une origine générique.
- Testez `OPTIONS` les demandes avant le vol séparément de la méthode d'application.
- Authentifiez et autorisez chaque demande protégée. Le CORS n'est pas un contrôle d'authentification.

Limitations du streaming et du protocole

Les fonctions Web transmettent les corps des demandes à votre application au fur et à mesure qu'ils arrivent et retransmettent les réponses au client HTTP/1.1. Le chemin de la demande est semi-duplex : Lambda transmet le corps complet de la demande avant de fournir la réponse de votre application. Lisez le corps de la demande dans son intégralité avant de rédiger la réponse. Réglé `timeoutSeconds` pour couvrir le streaming dans les deux sens : réception du corps de la demande et envoi de la réponse. Lorsque le délai est écoulé, Lambda met fin à la réponse. Le client reçoit le code de statut déjà envoyé, avec un corps tronqué. Arrêtez le travail en amont lorsque le client se déconnecte.

Lambda ne prend pas en charge WebSocket les mises à niveau. Lambda supprime les en-têtes de mise à niveau spécifiques à la connexion avant de transférer la demande. Utilisez des événements envoyés par le serveur lorsque le streaming unidirectionnel de serveur à client est suffisant.

Pour le contrat complet d'en-tête et de méthode, voirthe section called “Comportement HTTP”.

Connectivité sortante

Vous choisissez le chemin du réseau sortant pour chaque révision.

- Sans connecteur réseau de sortie : la révision atteint directement les `IPv4` destinations publiques sans passer par votre VPC. L'adresse source est Lambda-managed, n'est pas stable et ne convient pas à une liste d'autorisations. La révision n'a aucune route vers les ressources privées de votre VPC.
- Avec un connecteur réseau de sortie : la révision envoie le trafic sortant via des interfaces réseau élastiques situées dans les sous-réseaux du connecteur. Vos tables de routage, groupes de sécurité et listes de contrôle d'accès réseau (ACL) VPC s'appliquent. Utilisez cette option pour accéder à des ressources VPC privées, à des réseaux locaux connectés via un VPN Direct Connect ou à des destinations nécessitant du trafic provenant de votre espace d'adressage.

Le référencement d'un connecteur remplace le chemin sortant par défaut. Un connecteur place le trafic dans votre VPC, mais il ne fournit pas d'accès à Internet. Pour atteindre des `IPv4` destinations publiques, les sous-réseaux du connecteur ont besoin d'une route vers une passerelle NAT. Pour atteindre des `IPv6` destinations publiques, ils ont besoin d'un itinéraire vers une passerelle Internet de sortie uniquement.

Il n'existe aucune adresse IP source stable pour le trafic du connecteur. Configurez les groupes de sécurité de destination pour autoriser les groupes de sécurité du connecteur. Si une destination ne prend pas en charge les références aux groupes de sécurité, autorisez les blocs CIDR du sous-réseau du connecteur au lieu d'une adresse individuelle.

Lambda exécute les opérations de connecteur de manière asynchrone. Un connecteur indique `PENDING` lorsque Lambda crée ses interfaces réseau et `ACTIVE` quand les révisions peuvent y faire référence. Les autres états incluent `INACTIVE`,`FAILED`,`DELETING`, et`DELETE_FAILED`.

Après une mise à jour`InProgress`, `LastUpdateStatus` recherchez`Successful`, ou`Failed`. Si une opération échoue, utilisez le motif de l'état et le code du motif pour identifier le sous-réseau, le groupe de sécurité, les autorisations ou la capacité de l'adresse IP concernés.

Résolution DNS

Pour les noms DNS privés, activez le support DNS et les noms d'hôte DNS dans le VPC du connecteur. Associez toutes les zones hébergées privées Route 53 requises à ce VPC.

Chaque environnement d'exécution met en cache les réponses DNS. Après avoir modifié un enregistrement DNS, les environnements existants continuent d'utiliser l'ancienne réponse jusqu'à ce que la valeur mise en cache expire ou que Lambda remplace l'environnement. Pour forcer un déploiement impeccable, créez une nouvelle révision et transférez le trafic des terminaux vers celle-ci.

Lors du dépannage, testez séparément la résolution des noms et l'accessibilité au réseau. Connectez-vous à une destination par adresse IP pour vérifier le chemin réseau, puis testez son nom DNS.

Connexion d'une fonction Web à votre VPC

Un connecteur réseau de sortie est une ressource Lambda réutilisable. Vous créez le connecteur une seule fois et vous référencez une version publiée du connecteur à partir de chaque révision de fonction Web nécessitant un accès VPC.

Pour les fonctions Web, la référence du connecteur possède les propriétés suivantes :

- Une révision fait référence à zéro ou à un connecteur.
- L'ARN du connecteur doit inclure un qualificatif de version.
- Le connecteur doit se trouver dans le même AWS compte et dans la même région que la fonction Web.
- Le connecteur doit avoir `WebFunction` comme type de ressource de calcul associé.
- Seul un `HomeRegion` point de terminaison prend en charge les révisions qui font référence à un connecteur réseau de sortie.
- Vous ne pouvez pas modifier la référence une fois que vous l'avez définie. Pour l'ajouter, le modifier ou le supprimer, créez une nouvelle révision.

Conditions préalables

Avant de créer le connecteur :

- Choisissez au moins deux sous-réseaux dans différentes zones de disponibilité avec des adresses IP disponibles.
- Choisissez les groupes de sécurité qui autorisent le trafic sortant requis.
- Autorisez le trafic entrant en provenance des groupes de sécurité du connecteur sur chaque destination.
- Configurez les itinéraires depuis les sous-réseaux du connecteur vers les destinations privées, locales ou publiques requises.
- Créez un rôle d'opérateur qui accorde à Lambda l'autorisation de gérer les interfaces réseau.
- Assurez-vous que l'identité qui crée le connecteur et la révision possède les autorisations nécessairesthe section called “Autorisations pour configurer le réseau”, y compris `lambda:PassNetworkConnector` sur le connecteur et `iam:PassRole` sur le rôle d'opérateur.

Le rôle d'opérateur du connecteur et le rôle d'exécution de la révision ont des objectifs différents. Le rôle d'opérateur gère les interfaces réseau de votre VPC. Le rôle d'exécution autorise votre application à appeler AWS des API. Vous n'ajoutez pas d'autorisations d'interface réseau du connecteur au rôle d'exécution.

Autorisations relatives au rôle d'opérateur

Lambda assume le rôle d'opérateur du connecteur pour gérer les interfaces réseau du connecteur. La politique de confiance du rôle doit permettre au principal du service Lambda de `lambda.amazonaws.com` l'assumer :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Associez une politique d'autorisation telle que la suivante au rôle d'opérateur du connecteur. Cette politique permet à Lambda de créer et de baliser les interfaces réseau du connecteur :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CreateENI",
      "Effect": "Allow",
      "Action": "ec2:CreateNetworkInterface",
      "Resource": [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid": "TagENI",
      "Effect": "Allow",
      "Action": "ec2:CreateTags",
      "Resource": "arn:aws:ec2:*:*:network-interface/*",
      "Condition": {
        "StringEquals": {
```

```
          "ec2:ManagedResourceOperator": "network-connectors.lambda.amazonaws.com"
        }
      }
    }
  ]
}
```

Création d'un connecteur

La AWS CLI commande suivante crée un `IPv4` connecteur pour Web Functions. Remplacez le nom du connecteur, les ID de sous-réseau, l'ID du groupe de sécurité et l'ARN du rôle d'opérateur par vos propres valeurs.

```
aws lambda-core create-network-connector \
  --name my-connector \
  --configuration '{
    "VpcEgressConfiguration": {
      "SubnetIds": [
        "subnet-0ab1c2d3e4f5a6b78",
        "subnet-1bc2d3e4f5a6b7c89"
      ],
      "SecurityGroupIds": ["sg-0123456789abcdef0"],
      "NetworkProtocol": "IPv4",
      "AssociatedComputeResourceTypes": ["WebFunction"]
    }
  }' \
  --operator-role arn:aws:iam::123456789012:role/NetworkConnectorOperatorRole
```

Un connecteur prend en charge un type de ressource de calcul. Un connecteur pour Web Functions ne prend pas en charge un autre type de calcul Lambda, et son type de ressource de calcul est immuable.

Lambda crée le connecteur de manière asynchrone. Utilisez cette `get-network-connector` option pour attendre que ce `State` soit `ACTIVE` le cas et notez le numéro de version actuel.

Référencer le connecteur à partir d'une révision

`serviceConfig.egressNetworkConnectorArn`Défini lorsque vous créez la première révision de la fonction Web ou une révision ultérieure. Utilisez un ARN qualifié par version :

```
arn:aws:lambda:us-east-1:123456789012:network-connector:nc-0a1b2c3d4e5f6a7b8:4
```

La AWS CLI commande suivante crée une révision qui fait référence à la version 4 du connecteur. Remplacez le nom de la fonction, l'ARN du rôle d'exécution, l'ARN du connecteur et la région par vos propres valeurs.

```
aws lambda-web create-web-function-revision \
  --function-name my-web-function \
  --build-config file://build-config.json \
  --service-config '{
    "executionRoleArn": "arn:aws:iam::123456789012:role/WebFunctionExecutionRole",
    "timeoutSeconds": 30,
    "egressNetworkConnectorArn": "arn:aws:lambda:us-east-1:123456789012:network-
connector:nc-0a1b2c3d4e5f6a7b8:4"
  }' \
  --region us-east-1
```

Un ARN, un nom de connecteur ou un ID de connecteur non qualifié ne sont pas acceptés lors d'une révision. Après avoir créé la révision :

- Attendez que l'état de la révision soit atteint`Active`.
- Lisez la révision et confirmez qu'elle `egressNetworkConnectorArn` contient la version de connecteur attendue.
- Vérifiez que le point de terminaison achemine le trafic vers la révision. Un `HomeRegion` point de terminaison en `LatestRevision` mode récupère automatiquement la dernière révision active. Pour un point de terminaison en `Disabled` mode, mettez à jour ses pondérations de révision.
- Testez une destination VPC et confirmez le trafic à l'aide des journaux de flux VPC.

Le mode de déploiement automatique du terminal détermine si la création d'une révision active met automatiquement à jour le routage. Dans tous les modes, vérifiez quelle version est diffusée avant de tester son connecteur.

Mettre à jour ou supprimer la connectivité VPC

La mise à jour d'un connecteur entraîne la publication d'une nouvelle version. Les révisions existantes restent associées à la version dans l'ARN de leur connecteur.

Pour effectuer un changement de connecteur, procédez comme suit :

- Mettez à jour le connecteur avec`update-network-connector`. Le connecteur doit êtreACTIVE. Fournissez l'intégralité`VpcEgressConfiguration`, y compris tous les ID de sous-réseau et de

groupe de sécurité que vous souhaitez conserver, car la mise à jour remplace la configuration existante.

- Attendez que le connecteur `LastUpdateStatus` devienne`Successful`.
- Procurez-vous la nouvelle version du connecteur.
- Créez une révision qui fait référence à l'ARN qualifié pour la nouvelle version.
- Pour un `HomeRegion` point de terminaison en `LatestRevision` mode, vérifiez qu'il a bien pris en compte la nouvelle révision active. Pour un point de terminaison en `Disabled` mode, déplacez le trafic en mettant à jour ses pondérations de révision.

La mise à jour du connecteur sans créer de révision faisant référence à sa nouvelle version ne modifie pas la configuration réseau des fonctions Web en cours d'exécution.

Pour supprimer la connectivité VPC, créez une révision sans. `egressNetworkConnectorArn` Un `HomeRegion` point de terminaison en `LatestRevision` mode le récupère lorsqu'il devient actif. Pour un point de terminaison en `Disabled` mode, déplacez le trafic en mettant à jour ses pondérations de révision. La nouvelle révision utilise une `IPv4` sortie Lambda-managed publique et ne dispose plus d'un accès VPC privé.

> **Note**
>
> Avant de supprimer un connecteur réseau de sortie, éloignez le trafic du point de terminaison de chaque révision de fonction Web qui fait référence à une version du connecteur, puis supprimez ces révisions. La suppression d'un connecteur alors qu'une révision active y fait toujours référence interrompt la connectivité réseau pour les environnements d'exécution existants et nouveaux desservant cette révision.

Prise en charge d’IPv6

Le chemin sortant par défaut et un support de `IPv4` connecteur `IPv4` uniquement. Pour l'utiliser`IPv6`, configurez le connecteur avec la `NetworkProtocol` valeur définie sur`DualStack`.

Pour une connectivité à double pile :

- Les sous-réseaux du VPC et du connecteur doivent comporter `IPv6` des blocs CIDR.
- Les tables de routage doivent contenir des itinéraires pour les `IPv6` destinations requises.
- Les groupes de sécurité et les ACL réseau doivent autoriser `IPv6` le trafic.

- `IPv6`L'accès public nécessite une route : :/0 vers une passerelle Internet de sortie uniquement.
- Référencez la version du connecteur créée lorsque vous avez mis à jour le connecteur vers`DualStack`.

Ne déterminez pas `IPv6` la disponibilité en inspectant les interfaces au sein d'un environnement d'exécution. Vérifiez-le en établissant une `IPv6` connexion à partir du code de l'application et en consultant les journaux de flux VPC.

Comportement de dimensionnement pour Lambda Web Functions

Lambda adapte automatiquement le point de terminaison de votre fonction Web à mesure que le trafic arrive. Il est évolutif en deux dimensions :

- Nombre d'environnements — Lambda ajoute des environnements d'exécution supplémentaires, jusqu'à `maxEnvironments`.
- Demandes simultanées par environnement — Chaque environnement gère plusieurs demandes à la fois. Lambda gère une limite de simultanéité dynamique par environnement en fonction de votre utilisation des ressources. Vous contrôlez la limite supérieure de cette limite dynamique en utilisant `maxConcurrencyPerEnvironment`. Pour plus d'informations, consultez the section called “Limite de simultanéité dynamique par environnement”.

Vous pouvez également définir `rateLimit` sur un terminal pour limiter le taux d'arrivée de ses demandes. Il s'agit d'un paramètre facultatif qui est appliqué avant que les demandes n'atteignent vos environnements.

Un point de terminaison évolue à partir de zéro. Lorsqu'il n'y a pas de trafic, Lambda n'exécute aucun environnement. Cette page explique les paramètres de dimensionnement d'un terminal, les quotas de comptes associés et comment choisir des valeurs qui optimisent les coûts ou les performances.

Environnements d'exécution

Un environnement d'exécution est une instance de calcul isolée qui exécute votre serveur HTTP. Chaque environnement possède sa propre mémoire, son propre système de fichiers et son propre espace de traitement. Pour savoir comment Lambda initialise, réutilise et arrête un environnement d'exécution, voir the section called “Cycle de vie environnemental”.

Lambda crée et supprime des environnements automatiquement en fonction du trafic :

- Lorsque le trafic augmente, Lambda crée des environnements supplémentaires pour répondre à la demande de trafic.
- Lorsque le trafic diminue, Lambda vide les environnements sous-utilisés et les supprime.
- Lorsqu'il n'y a pas de trafic, Lambda supprime tous les environnements. Le point final passe à zéro.

Il n'y a pas de réglage d'environnement minimal ou réservé. Un point de terminaison repart toujours de zéro à mesure que le trafic arrive. Pour éviter les démarrages à froid en cas de faible augmentation du trafic, Lambda adapte automatiquement les environnements d'exécution avant la demande afin de maintenir la capacité inutilisée (headroom) pour le trafic entrant. Lorsque les environnements sont sous-utilisés, Lambda les réduit, y compris jusqu'à zéro.

Limite de simultanéité dynamique par environnement

La limite de simultanéité dynamique par environnement est Lambda-managed limite le nombre de requêtes qu'un seul environnement d'exécution gère simultanément. En fonction de l'utilisation des ressources de votre fonction, Lambda ajuste automatiquement cette limite pour optimiser l'efficacité et les performances. Lambda étend les nouveaux environnements lorsque les environnements existants sont proches de leurs limites. Lorsque la limite empêche tous les environnements existants d'accepter davantage de demandes, les demandes sont mises en file d'attente, en attendant le prochain environnement disponible.

Pour une nouvelle fonction Web, Lambda définit une limite de départ prudente et l'ajuste rapidement en fonction de l'utilisation des ressources de la fonction. Pour plus d'informations sur la façon dont la limite change lors de la gestion de la charge, voir the section called “Limite de simultanéité dynamique d'une nouvelle fonction Web”.

Vous ne configurez pas directement la limite dynamique. Au lieu de cela, vous pouvez lui appliquer une limite supérieure en définissant `maxConcurrencyPerEnvironment` sur la révision. La limite dynamique de Lambda peut être inférieure à cette valeur, mais ne la dépasse jamais. Par exemple, si vous définissez `maxConcurrencyPerEnvironment` à 32, Lambda achemine au maximum 32 requêtes simultanées vers n'importe quel environnement, même si celui-ci est capable d'en traiter davantage.

La plupart des applications peuvent s'appuyer sur la limite dynamique sans changer `maxConcurrencyPerEnvironment`. Pour savoir quand le modifier, consultez the section called “Choix des paramètres de dimensionnement”.

Paramètres de dimensionnement

Trois paramètres contrôlent la façon dont Lambda fait évoluer votre fonction Web. Vous configurez chaque paramètre soit sur le point de terminaison, soit sur la révision.

Paramètre	Configuré sur	Plage valide	Par défaut	Description
`maxConcurrencyPerEnvironment`	Révision	1 à 128	64	La limite supérieure du Lambda-managed limite de simultanéité dynamique par environnement. Lambda ajuste automatiquement la simultanéité réelle par environnement, de sorte que la plupart des applications peuvent s'appuyer sur la limite dynamique sans modifier cette valeur.
`maxEnvironments`	Endpoint	Facultatif. 2 à 10 000	Aucune	Limite le nombre d'environnements d'exécution pour le terminal dans chacun Région AWS. Contrôle l'échelle horizontale. La mise à l'échelle de l'environnement des terminaux est toujours limitée par le quota de processeurs virtuels du compte disponible, même si `maxEnvironments` n'est pas défini.
`rateLimit`	Endpoint	Facultatif. 0 à 10 000	Aucune	Limite le taux d'arrivée des demandes du terminal, en demandes par seconde, dans chaque Région AWS. Les valeurs inférieures à 1 000

Paramètre	Configuré sur	Plage valide	Par défaut	Description
				doivent être un multiple de 100 et les valeurs supérieures à 1 000 doivent être un multiple de 1 000. La valeur 0 bloque tout le trafic. Les requêtes dépassant la limite de débit effective reçoivent une réponse HTTP 429 (Too Many Requests). Lorsqu'il n'est pas défini, le taux d'arrivée du terminal est limité par le quota tarifaire par compte par point de terminaison.

`maxEnvironments` et `rateLimit` sont des propriétés de point de terminaison facultatives. Vous pouvez les mettre à jour sans créer de nouvelle révision. Par défaut, aucun des deux n'est défini. Un grand `maxEnvironments` ne garantit pas que le terminal puisse évoluer aussi loin. La mise à l'échelle de l'environnement est toujours limitée par le quota régional de processeurs virtuels du compte. UNE `rateLimit` de 0 bloque tout le trafic. Pour plus de détails, consultez the section called “Étranglement”. Le taux de demandes des terminaux est toujours limité par le quota de taux de demandes du compte, même lorsque `rateLimit` n'est pas défini. Pour les quotas, voir la section suivante.

Pour changer `maxEnvironments` ou `rateLimit`, courir `aws lambda-web update-web-function-endpoint` avec le `--scaling-config` ou `--throttle-config` paramètre, par exemple `--scaling-config '{"maxEnvironments": 50}'` ou `--throttle-config '{"rateLimit": 8000}'`. Omettez un paramètre pour conserver sa valeur actuelle. Pour effacer une valeur que vous avez définie, transmettez un objet vide, tel que `--scaling-config '{}'`. Pour plus d'informations, voir the section called “Mise à jour d'un terminal”. `maxConcurrencyPerEnvironment` est un paramètre de révision. Pour le modifier, créez une nouvelle révision. Le fait que la nouvelle révision reçoive du trafic dépend du mode de déploiement automatique du terminal. Pour plus d’informations, consultez the section called “Création d'une révision”.

Quotas de comptes

Ces quotas s'appliquent par Région AWS. Elles s'appliquent toujours en plus des limites de points de terminaison que vous avez configurées en option.

- Per-endpoint limite de débit : 10 000 requêtes par seconde (RPS).
- Limite de débit totale du compte : 100 000 RPS sur tous les terminaux de la région.
- Limite de processeurs virtuels du compte : 2 000 processeurs virtuels sur tous les terminaux de la région. Chaque environnement d'exécution consomme 2 processeurs virtuels, ce quota limite donc le nombre total d'environnements par Région AWS sur l'ensemble du compte.

Pour connaître les valeurs de quota actuelles et savoir comment demander une augmentation, voir the section called “Fonctions Web Lambda”.

Comment les paramètres de dimensionnement interagissent

Ces trois paramètres de dimensionnement fonctionnent indépendamment pour déterminer l'échelle de votre terminal. À l'exception des quotas de comptes, chaque point de terminaison évolue indépendamment, même les terminaux appartenant à la même fonction Web.

Capacité de simultanéité totale

Vous pouvez considérer que le nombre maximal de demandes en vol du terminal est d'environ `maxEnvironments` multiplie par la limite de simultanéité dynamique par environnement que Lambda autorise actuellement. Le maximum que le terminal peut gérer à la fois est `maxEnvironments` × `maxConcurrencyPerEnvironment`. Il n'atteint ce chiffre que lorsqu'il fonctionne `maxEnvironments` environnements et chacun gère `maxConcurrencyPerEnvironment` demandes. Si `maxEnvironments` n'est pas défini, le terminal évolue pour répondre à la demande, dans la limite du quota de processeurs virtuels du compte.

Limite du taux de demande total

`rateLimit` limite les demandes par seconde, indépendamment de la capacité de simultanéité. Lambda renvoie le protocole HTTP 429 pour les requêtes supérieures à la limite de débit, même lorsque les environnements ont la capacité de les traiter.

Mise à l'échelle

Avant que tous les environnements n'atteignent la limite de simultanéité dynamique, Lambda étend d'autres environnements, jusqu'à `maxEnvironments`. Un point de terminaison cesse de croître lorsqu'il atteint `maxEnvironments` ou le quota de processeur virtuel du compte. Si un endpoint n'est pas en mesure d'évoluer et que tous les environnements existants sont pleinement utilisés, Lambda limite immédiatement les nouvelles demandes avec une réponse HTTP 429 (Too Many Requests). Lambda ne met pas en file d'attente les requêtes limitées. Si un nouvel environnement d'exécution est en cours d'initialisation, les requêtes sont mises en file d'attente au lieu d'être limitées immédiatement.

Dépassement temporaire

Lors de changements de poids de révision, de cycles internes de la flotte et d'autres événements opérationnels, Lambda peut temporairement dépasser `maxEnvironments` pour prioriser la disponibilité. Ce dépassement est bref et Lambda revient automatiquement à la limite configurée. Vous n'avez pas à prévoir de budget pour ces événements opérationnels lorsque vous le souhaitez `maxEnvironments`.

Example Exemple : calcul de capacité

Vous configurez les paramètres suivants pour votre fonction Web :

- `maxEnvironments` = 10
- `maxConcurrencyPerEnvironment` = 64
- `rateLimit` = 8 000

Ces paramètres limitent la simultanéité (demandes en cours en même temps) et le taux de demandes (demandes acceptées par seconde) séparément. Avec jusqu'à 10 environnements et jusqu'à 64 demandes simultanées chacun, le terminal peut traiter au maximum 640 demandes simultanées (10 × 64). La limite dynamique étant souvent inférieure, la simultanéité soutenue est généralement moindre. La limite que le terminal atteint en premier dépend de la durée de chaque requête.

Concurrency-bound point de terminaison

Supposons que chaque requête prenne 200 ms, par exemple parce qu'elle attend une requête de base de données. Avec 640 requêtes en cours, le terminal traite au maximum environ 3 200 demandes par seconde (640 ÷ 0,2 s), ce qui est inférieur aux 8 000 RPS `rateLimit`. Lorsque

les 10 environnements sont pleinement utilisés, Lambda limite les nouvelles requêtes à l'aide du protocole HTTP 429. Pour augmenter le trafic, augmentez `maxEnvironments`.

Request-rate-bound point de terminaison

Supposons que chaque requête prenne 10 ms. À 8 000 requêtes par seconde, environ 80 requêtes sont en cours (8 000 × 0,01 s), bien en dessous de 640. Lambda renvoie le protocole HTTP 429 pour les requêtes supérieures à 8 000 RPS, même si les environnements ont la capacité de les traiter. Pour accepter plus de demandes, augmentez `rateLimit`, jusqu'au quota de 10 000 images par seconde par point final.

Étranglement

Lorsque le taux de demandes entrantes dépasse le `rateLimit` paramètre, Lambda renvoie une réponse HTTP 429 (Too Many Requests) pour les demandes excédentaires. La limite de débit s'applique au terminal dans son ensemble dans chaque Région AWS.

Lambda renvoie également une réponse HTTP 429 lorsque tous les environnements sont pleinement utilisés, soit parce que le point de terminaison a atteint `maxEnvironments` ou le compte a atteint son quota de processeur virtuel. Pour plus d'informations, consultez the section called “Comment les paramètres de dimensionnement interagissent”.

Lambda peut également renvoyer HTTP 429 avec le `Platform.EndpointConcurrentInitThrottle` type d'erreur lorsque trop d'environnements d'exécution s'initialisent en même temps. Cet accélérateur n'incrémente pas une métrique d'accélérateur. Pour les mesures que les autres types d'accélérateur incrémentent, voir the section called “Métriques”.

Lorsqu'un point de terminaison est `rateLimit` vaut 0, Lambda renvoie HTTP 503 (Service non disponible) au lieu de HTTP 429, avec le `lambda-web-error-type` en-tête `Platform.EndpointDisabled`. Lambda peut également renvoyer le protocole HTTP 503 lorsqu'il supprime la charge pour protéger le service. Réessayez un 503 qui n'a pas `lambda-web-error-type` en-tête avec backoff et gigue. A 503 avec `Platform.EndpointDisabled` continue jusqu'à ce que vous définissiez `rateLimit` à une valeur non nulle.

Lambda mesure la limite de débit par seconde. De brèves rafales au-dessus de la limite peuvent être acceptées. Un trafic soutenu au-dessus de la limite entraîne un ralentissement.

Lorsque votre application reçoit des réponses HTTP 429, implémentez un backoff exponentiel avec gigue dans votre code client pour réessayer les requêtes limitées.

Mise à l'échelle et réduction

Mise à l'échelle ascendante

Lorsque le trafic augmente et que les environnements existants approchent de la limite de simultanéité dynamique par environnement, Lambda crée des environnements d'exécution supplémentaires. Chaque nouvel environnement s'initialise avant de répondre aux demandes. Pour les étapes d'initialisation et la limite de temps de démarrage, voir the section called “Initialisation (démarrage à froid)”.

Lors de l'initialisation d'un nouvel environnement, Lambda achemine les demandes vers les environnements existants qui disposent de la capacité disponible. Lorsqu'aucun environnement n'a de capacité, la demande est en attente pendant que Lambda en initialise un nouveau (démarrage à froid). Lambda renvoie HTTP 429 uniquement lorsque l'une des limites de the section called “Étranglement” s'applique, comme `maxEnvironments` ou le quota de processeur virtuel du compte.

Réduire

Lorsque le trafic diminue, Lambda identifie les environnements sous-utilisés et les supprime. Lambda vide un environnement avant de le supprimer. Il arrête d'acheminer les nouvelles demandes vers l'environnement, permet aux demandes en cours de traitement de se terminer dans les meilleurs délais et envoie `SIGTERM`. Pour plus de détails, consultez the section called “Cycle de vie environnemental”.

Lambda passe à zéro environnement lorsqu'il n'y a pas de trafic. La requête suivante lance un nouvel environnement (démarrage à froid).

Choix des paramètres de dimensionnement

Tenez compte des éléments suivants lorsque vous choisissez des valeurs pour le point de terminaison `rateLimit`, point final `maxEnvironments`, et révision `maxConcurrencyPerEnvironment`.

En choisissant `rateLimit`

> La valeur par défaut est none, ce qui signifie que le taux de demandes d'un terminal est limité à la fois par le quota RPS de 10 000 par terminal et par le quota RPS de 100 000 comptes. Envisagez de définir un `rateLimit` valeur lorsque vous souhaitez limiter le montant qu'un terminal peut réclamer sur le quota RPS de votre compte, qui est partagé par tous vos terminaux.

Réglage d'un `rateLimit` peut également être utile pour limiter le trafic total aux dépendances en aval.

En choisissant `maxEnvironments`

La valeur par défaut est none, ce qui signifie que le nombre d'environnements d'un terminal est uniquement limité par le quota de processeurs virtuels du compte. Envisagez de définir un `maxEnvironments` valeur lorsque vous souhaitez limiter le montant qu'un terminal peut réclamer sur le quota de processeurs virtuels de votre compte, qui est partagé par tous vos terminaux.

Lors de la configuration d'un `maxEnvironments` valeur, pensez à surveiller le nombre d'environnements du terminal afin d'être alerté lorsqu'il se trouve à proximité de votre `maxEnvironments` limite, et prenez des mesures pour éviter la limitation pour une application qui connaît une croissance organique au fil du temps.

Régler une valeur faible de `maxEnvironments` peut vous aider à limiter le coût de fonctionnement des environnements de votre terminal. Envisagez d'utiliser une valeur faible pour les projets de loisirs non critiques.

En choisissant `maxConcurrencyPerEnvironment`

Une révision `maxConcurrencyPerEnvironment` est la limite supérieure de la limite de simultanéité dynamique gérée par environnement de Lambda. La valeur par défaut est 64 et la plupart des utilisateurs ne devraient pas avoir à sélectionner une valeur optimale.

Pour les applications dont la mémoire est limitée, paramétrer `maxConcurrencyPerEnvironment` une valeur inférieure à la valeur par défaut peut permettre d'obtenir un comportement plus prévisible.

Pour CPU-bound applications, réglage `maxConcurrencyPerEnvironment` une valeur inférieure à la valeur par défaut peut réduire la contention du processeur et améliorer la latence en régime permanent dans les environnements chauds, mais peut également entraîner des démarrages à froid plus fréquents. Réglage `maxConcurrencyPerEnvironment` une valeur supérieure à la valeur par défaut n'aura probablement aucun effet si la limite de simultanéité dynamique gérée par Lambda limite le trafic vers l'environnement.

Pour I/O-bound applications, réglage `maxConcurrencyPerEnvironment` une valeur supérieure à la valeur par défaut peut améliorer l'utilisation par environnement et réduire les coûts.

Surveillez les éléments suivants CloudWatch des mesures pour déterminer si vos paramètres de dimensionnement sont appropriés. Pour les définitions des métriques, voir the section called “Métriques”.

- `EndpointRequestThrottles` et `AccountRequestThrottles` — Si `EndpointRequestThrottles` est constamment supérieur à zéro, augmente `rateLimit`, jusqu'au quota par terminal de 10 000 RPS. `AccountRequestThrottles` augmente lorsque le compte atteint son quota de demandes dans la Région. Pour réduire ces contraintes, demandez une augmentation ou une diminution du quota `rateLimit` sur d'autres points de terminaison.
- `EndpointActiveEnvironmentThrottles` et `AccountActiveVCPUArm64Throttles` — Ces métriques s'incrémentent lorsque `maxEnvironments` ou le quota de processeur virtuel du compte empêche toute augmentation supplémentaire de la capacité d'exploitation. Pour réduire ces gaz, augmentez `maxEnvironments` ou demandez une augmentation du quota du processeur virtuel.
- `EndpointActiveEnvironments` et `EnvironmentConcurrentRequests` — Si les environnements actifs approchent `maxEnvironments`, ou les demandes simultanées par environnement restent proches `maxConcurrencyPerEnvironment`, augmentez le paramètre approprié.
- Latence des applications : mesurez la latence à l'aide d'une métrique d'application, à partir de journaux structurés ou à l'aide des mesures de latence de votre porte d'entrée. Si la latence augmente à mesure que la simultanéité par environnement augmente, réduisez `maxConcurrencyPerEnvironment` pour réduire les conflits par environnement et répartir la charge sur un plus grand nombre d'environnements.

Mise à l'échelle pour MultiRegion et PerRegion points finaux

Pour les fonctions Web avec MultiRegion ou PerRegion points de terminaison, les paramètres de mise à l'échelle s'appliquent indépendamment à chaque Région AWS où le terminal fonctionne.

Chaque région crée et gère son propre pool d'environnements d'exécution. Le trafic d'une région ne consomme pas la capacité de mise à l'échelle d'une autre région.

Exemples de dimensionnement

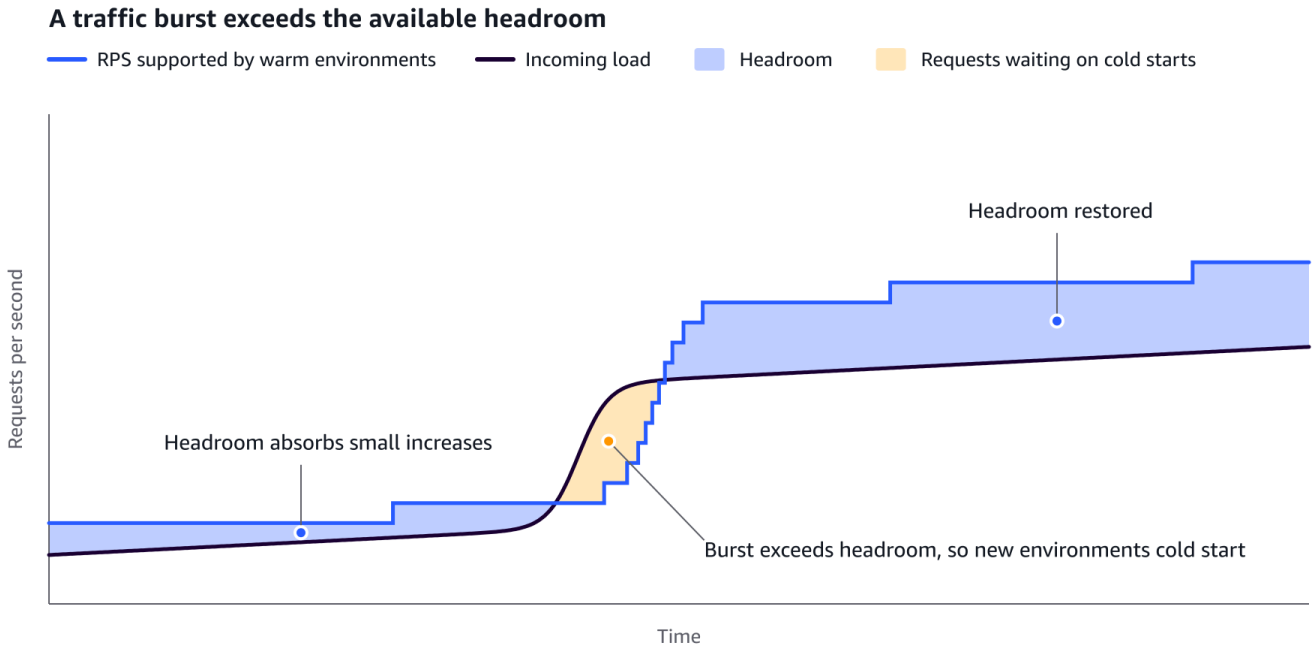
Lambda fait évoluer votre terminal pour maintenir une marge de manœuvre supérieure à sa charge actuelle. La marge de manœuvre est la différence entre la charge de demandes entrantes et la charge de demandes totale que les environnements d'exécution chauds peuvent prendre en charge. Il absorbe les petites augmentations de trafic sans attendre le démarrage de nouveaux

environnements. La capacité augmente progressivement, car chaque nouvel environnement n'ajoute de la capacité qu'une fois son initialisation terminée. Lorsque le terminal atteint une limite, la capacité cesse de croître et Lambda limite les demandes qui dépassent ce que le terminal peut accepter.

Les exemples suivants montrent comment le point de terminaison gère une rafale de trafic, comment la limite de simultanéité dynamique par environnement change lors des tests de charge sur une nouvelle fonction Web et comment le point de terminaison se comporte lorsque la charge atteint chaque type de limite. Les graphiques illustrent le comportement général et ne sont pas dessinés à l'échelle.

Gérer une rafale de trafic

Lorsque la charge augmente progressivement, la marge de manœuvre absorbe l'augmentation tandis que Lambda adapte de nouveaux environnements en arrière-plan. Lorsque la charge augmente plus rapidement que la hauteur libre ne peut absorber, les environnements chauds ne peuvent pas gérer toutes les demandes entrantes. Lambda démarre de nouveaux environnements pour gérer la charge dépassant la marge de manœuvre, et ces requêtes attendent que les nouveaux environnements démarrent à froid. Une fois les nouveaux environnements prêts, Lambda rétablit la marge au-dessus de la nouvelle charge.

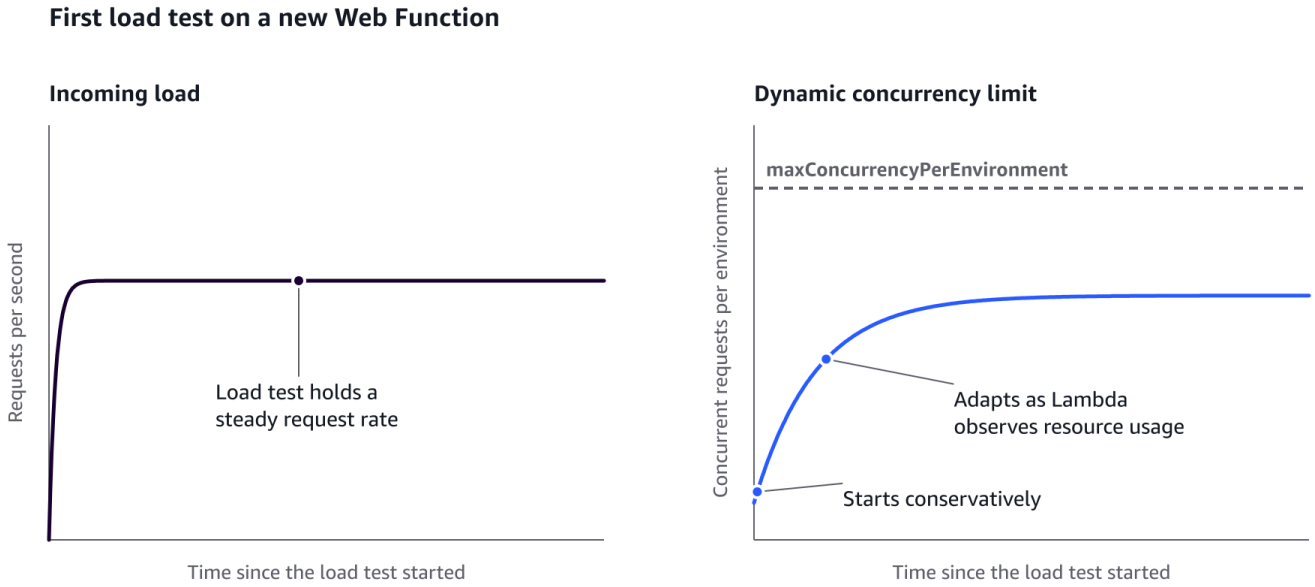


Limite de simultanéité dynamique d'une nouvelle fonction Web

La limite de simultanéité dynamique par environnement commence de manière prudente pour une nouvelle fonction Web. Au fur et à mesure que la fonction gère le trafic, Lambda apprend de son

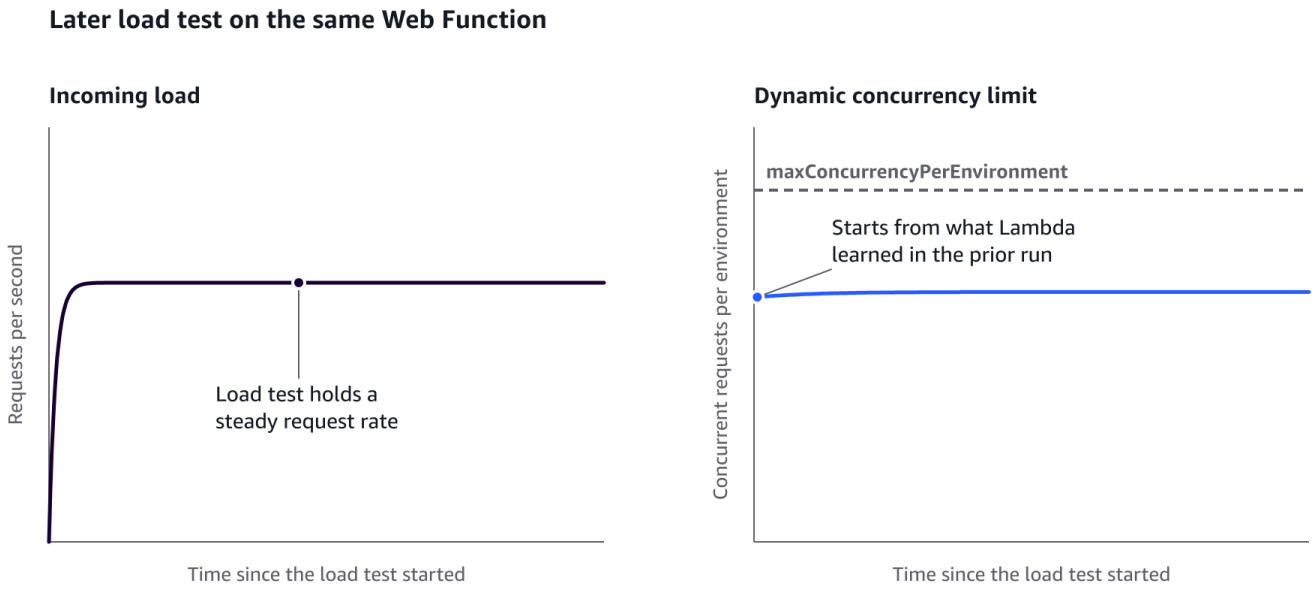
utilisation des ressources et ajuste la limite. Lambda mémorise ce qu'il a appris lorsque la fonction passe à zéro, de sorte que les environnements qui démarrent plus tard bénéficient d'un trafic plus précoce.

Les graphiques suivants montrent le premier test de charge sur une nouvelle fonction Web. La charge entrante augmente rapidement pour atteindre un taux de demandes constant et le maintient. La limite de simultanéité dynamique commence à être faible, augmente à mesure que Lambda l'ajuste en fonction de l'utilisation des ressources de la fonction, puis se stabilise en dessous `maxConcurrencyPerEnvironment`.



Comme Lambda se souvient de ce qu'il a appris lors du trafic précédent, les tests de charge ultérieurs sur la même fonction Web ne démarrent pas de manière conservatrice.

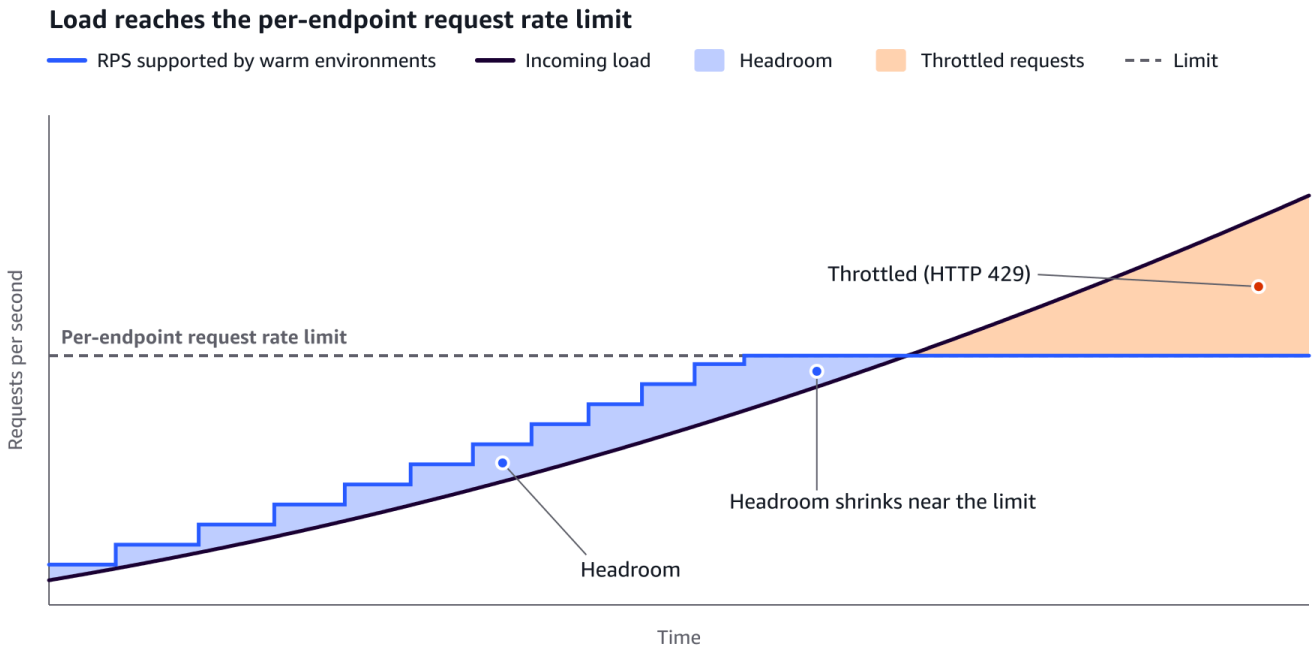
Les graphiques suivants montrent un test de charge ultérieur sur la même fonction Web. La charge entrante atteint le même taux de demandes constant, et la limite de simultanéité dynamique commence au niveau que Lambda a appris lors de l'exécution précédente.



Comme la limite commence de manière prudente, le premier test de charge d'une nouvelle fonction Web peut utiliser davantage d'environnements d'exécution que les exécutions ultérieures. Pour mesurer les performances auxquelles votre fonction peut s'attendre en cas de trafic constant, exécutez le test de charge plusieurs fois et utilisez les résultats des exécutions ultérieures.

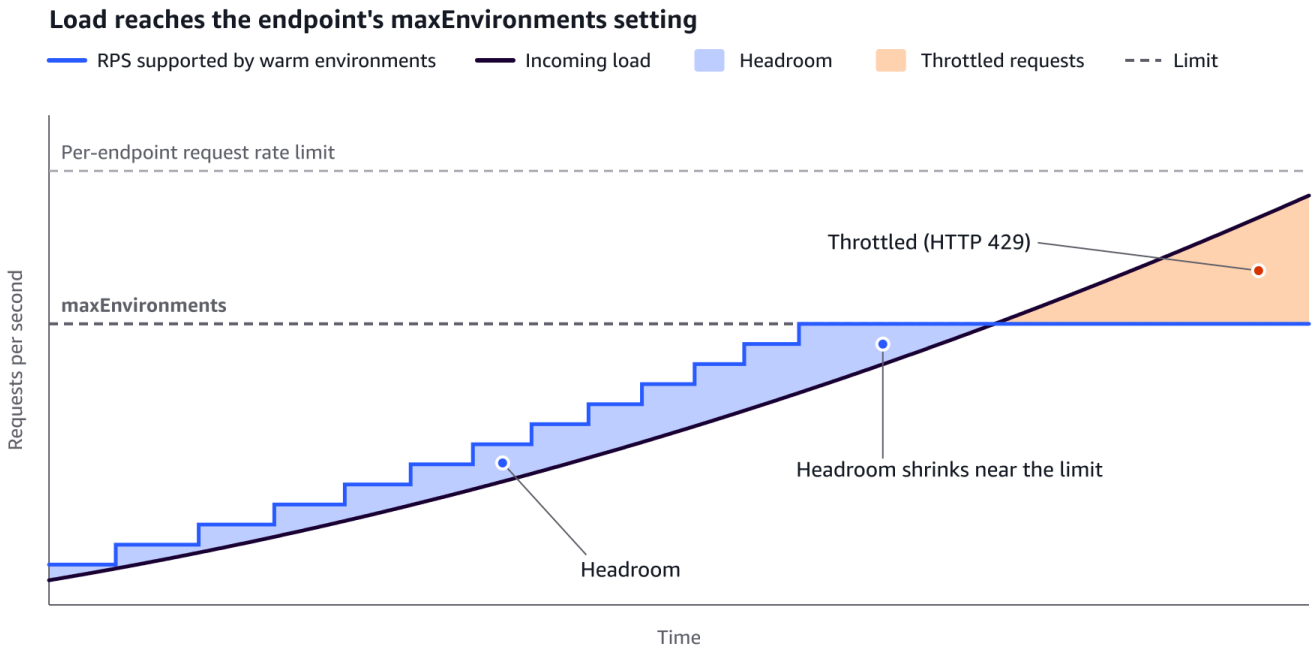
Atteindre la limite de taux de demandes par point de terminaison

La limite de débit de demandes limite la charge que le terminal peut accepter, afin que la capacité ne dépasse pas cette limite. Lorsque la charge approche du quota de taux par point de terminaison ou `rateLimit` réglage, la hauteur libre diminue. Lorsque la charge dépasse la limite, Lambda renvoie HTTP 429 pour les requêtes supérieures à cette limite. Pour accepter plus de demandes, augmentez `rateLimit`, jusqu'au quota de taux par point de terminaison.



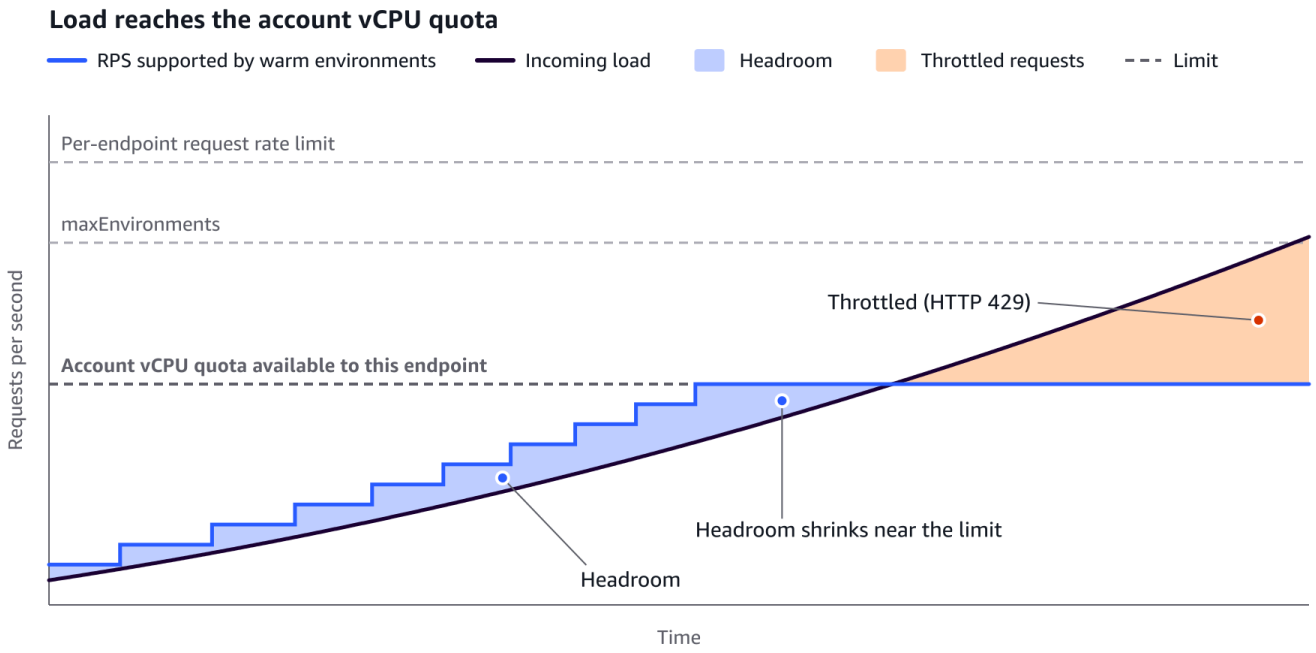
Atteindre MaxEnvironments

Dans cet exemple, `maxEnvironments` est inférieur à la limite de débit de demandes. Quand le point final atteint `maxEnvironments`, Lambda arrête d'ajouter des environnements d'exécution. La charge peut continuer à augmenter, ce qui entraîne une diminution de la hauteur libre. Lorsque la charge dépasse ce que les environnements peuvent gérer, Lambda limite les nouvelles requêtes avec le protocole HTTP 429, même si le taux de demandes est toujours inférieur à la limite de débit. Pour augmenter la capacité, augmentez `maxEnvironments`.



Atteindre le quota de processeur virtuel du compte

Tous les terminaux d'un compte partagent le quota de processeur virtuel dans chacun Région AWS. Les environnements utilisés par d'autres terminaux réduisent la capacité d'évolutivité de ce terminal. Dans cet exemple, le quota de processeur virtuel disponible pour le terminal est inférieur à la fois à ses `maxEnvironments` réglage et sa limite de débit de demandes. Lorsque le compte atteint le quota, Lambda arrête d'ajouter des environnements et limite les demandes qui dépassent la capacité disponible, même si le terminal n'a pas atteint ses propres limites. Pour augmenter la capacité, demandez une augmentation du quota du processeur virtuel.



Cycle de vie des environnements d'exécution

Un environnement d'exécution est une instance de calcul isolée qui exécute votre serveur HTTP. AWS Lambda crée des environnements d'exécution pour votre fonction Web Lambda lorsque le trafic arrive. Il achemine les demandes vers des environnements actifs et supprime les environnements qui ne sont plus nécessaires. Comprendre ce cycle de vie vous permet d'optimiser les performances de démarrage et d'écrire du code qui gère correctement l'initialisation et l'arrêt.

Phases du cycle de vie

Chaque environnement d'exécution passe par les phases suivantes :

Phase	Que se passe-t-il	Traitement des demandes
Initialisation	Lambda charge votre code, prépare le runtime et démarre le processus de votre serveur HTTP. Votre serveur doit commencer à écouter l'adresse `AWS_LAMBDA_HTTP_ENDPOINT` dans les 10 secondes.	L'environnement ne peut pas répondre aux demandes lors de l'initialisation.
Prêt	Votre serveur HTTP écoute et l'environnement est disponible pour recevoir des requêtes. Lambda achemine les demandes entrantes vers cet environnement.	L'environnement accepte les demandes dans la `maxConcurrencyPerEnvironment` limite maximale.
Arrêter	Lambda arrête d'acheminer les nouvelles demandes vers l'environnement, laisse les demandes en cours de traitement se terminer au mieux`SIGTERM`, envoie puis met fin à l'environnement.	Aucune nouvelle demande n'est acheminée vers l'environnement. In-flight les demandes peuvent continuer, mais leur achèvement n'est pas garanti. Ensuite`SIGTERM`, le processus dispose d'une seconde pour terminer le nettoyage. L'état du processus est perdu.

Initialisation (démarrage à froid)

Lorsque Lambda crée un nouvel environnement d'exécution, la phase d'initialisation inclut les étapes suivantes :

1. Lambda charge le code depuis votre package de déploiement .zip.
2. Lambda configure l'environnement d'exécution (y compris vos variables Node.js d'environnement).
3. Lambda lance votre processus de candidature.
4. Votre serveur HTTP commence à écouter sur l'hôte et le port spécifiés par la variable d'`AWS_LAMBDA_HTTP_ENDPOINT`environnement. Il doit commencer à écouter dans les 10 secondes.
5. Lambda détecte que votre serveur écoute et marque l'environnement comme étant prêt.

Un démarrage à froid se produit lorsque Lambda doit créer un nouvel environnement pour traiter une demande car aucun environnement n'est disponible. La première demande après un démarrage à froid subit une latence supplémentaire dès la phase d'initialisation. Les demandes ultérieures adressées au même environnement n'entraînent pas ce coût.

Pour réduire l'impact du démarrage à froid :

- Minimisez la taille de votre package de déploiement. Les petits paquets se chargent plus rapidement.
- Réduisez le temps de démarrage du serveur. Différez les initialisations lourdes (telles que le chargement de gros fichiers de données) jusqu'à ce que le serveur commence à écouter. Lambda achemine les requêtes vers l'environnement dès que le serveur les écoute, alors obligez les gestionnaires de demandes qui dépendent du travail différé à attendre la fin de celui-ci, par exemple en attendant une promesse partagée.
- Utilisez l'initialisation différée pour les connexions aux bases de données et les clients de services externes. Établissez des connexions à la première demande plutôt qu'au démarrage.

Scale-down et arrêt

Lambda surveille l'utilisation de l'environnement de votre point de terminaison et supprime les environnements inutiles, par exemple lorsque le trafic diminue. Avant de supprimer un environnement, Lambda utilise la séquence d'arrêt suivante :

1. Lambda arrête d'acheminer les nouvelles demandes vers l'environnement.
2. Lambda permet de traiter les demandes en vol dans les meilleures conditions.
3. Lambda envoie. `SIGTERM` Le processus dispose d'une seconde pour terminer le nettoyage avant que Lambda ne l'arrête et ne supprime l'environnement.

Lorsqu'il n'y a pas de trafic, Lambda adapte votre fonction Web à zéro environnement. La demande suivante après une période d'échelle allant jusqu'à zéro déclenche un nouveau démarrage à froid.

Si votre application doit effectuer un nettoyage pendant l'arrêt, faites-le. `SIGTERM` Le nettoyage doit être terminé dans un délai d'une seconde. Ne vous fiez pas à l'exécution de rappels d'arrêt, car Lambda ne peut garantir un arrêt progressif dans tous les modes de défaillance, par exemple en cas de panne matérielle sous-jacente.

L'exemple suivant gère `SIGTERM` :

```
process.on('SIGTERM', () => {
  // Finish short cleanup, such as flushing buffered logs, within 1 second.
  process.exit(0);
});
```

Réutilisation de l'environnement

Lambda réutilise les environnements d'exécution pour plusieurs requêtes afin d'éviter les démarrages à froid répétés. Un environnement unique peut répondre à des milliers de demandes au cours de sa durée de vie. Autrement dit :

- L'état global persiste : les variables, les caches et les connexions que votre serveur initialise au démarrage sont conservés dans toutes les demandes. Vous pouvez l'utiliser pour la mise en cache en mémoire ou le regroupement de connexions.
- L'état du système de fichiers persiste : les fichiers que votre code écrit dans le système de fichiers local (tels que`/tmp`) sont conservés jusqu'à ce que Lambda supprime l'environnement.
- Aucune durée de vie garantie : Lambda peut supprimer un environnement à tout moment. Ne vous fiez pas à un environnement qui dure pendant une certaine durée. Conservez les données importantes dans un magasin externe tel que DynamoDB ou Amazon S3.

Gestion des demandes simultanées

Chaque environnement d'exécution de fonction Web gère plusieurs requêtes HTTP simultanées. Le `maxConcurrencyPerEnvironment` paramètre de révision contrôle le nombre maximum de demandes simultanées par environnement.

Étant donné que votre serveur traite plusieurs demandes simultanément, votre code doit être sûr pour une utilisation simultanée :

- Ne stockez pas l'état de chaque demande dans des variables globales. Utilisez plutôt des variables limitées à la demande ou un contexte d'intergiciel.
- Protégez les états mutables partagés, tels que les caches ou les compteurs, que vous modifiez au-delà des limites. `await` Les demandes s'entrelacent dans la boucle d'événements. Si une séquence de lecture-modification-écriture couvre une opération asynchrone, une autre demande en cours de vol peut lire ou modifier l'état avant la fin de la séquence.

- Sachez qu'elle Node.js utilise une boucle d'événements à thread unique. CPU-intensive les opérations synchrones bloquent toutes les demandes simultanées dans cet environnement. Utilisez le mode asynchrone I/O et évitez de bloquer la boucle d'événements.

Pour plus d'informations sur les paramètres de simultanéité et l'optimisation, consultezthe section called “Mise à l’échelle”.

Runtimes des fonctions Web Lambda

Les fonctions Web Lambda exécutent le code de votre serveur HTTP à l'aide d'environnements d'exécution gérés. Votre application doit démarrer un serveur HTTP qui écoute sur l'hôte et le port spécifiés par la variable d'`AWS_LAMBDA_HTTP_ENDPOINT`environnement. Les fonctions Web Lambda sont actuellement prises en charge. Node.js Par défaut, le moteur d'exécution `index.js` se charge à la racine du package de déploiement. Pour utiliser un autre fichier d'entrée, définissez la variable d'`AWS_LAMBDA_NODEJS_ENTRYPOINT`environnement. Pour plus de détails, consultez the section called “Variables d’environnement”.

Pris en charge Node.js versions

Identifiant d'exécution	Version de l’Node.js	Statut
`nodejs24.x`	Node.js24	Pris en charge

Spécifiez l'identifiant d'exécution dans la `runtimeConfig` section lorsque vous créez une révision. Par exemple :

```
"runtimeConfig": { "runtime": "nodejs24.x" }
```

Le moteur d'exécution des fonctions `nodejs24.x` Web suit le même cycle d'obsolescence que le moteur d'exécution des fonctions d'événement Lambda correspondant. Pour les dates de dépréciation et le processus de dépréciation, voir. the section called “politique d’obsolescence de l’exécution”

Correctif automatique lors de l'exécution

Lambda corrige automatiquement le Node.js moteur d'exécution avec des mises à jour de sécurité et des corrections de bogues. Les correctifs s'appliquent à la couche d'exécution sous-jacente

et ne modifient pas le code de votre application. L'`runtime`identifiant de votre révision (par exemple,`nodejs24.x`) correspond toujours à la dernière version corrigée de ce moteur d'exécution majeur.

> **Note**
>
> Les contrôles de gestion d'exécution ne sont pas pris en charge pour les fonctions Web. Vous ne pouvez pas épingler une version de correctif spécifique ni désactiver l'application automatique de correctifs. Lambda utilise toujours la dernière version corrigée du moteur d'exécution que vous avez spécifié.

Pour plus d'informations sur la façon dont Lambda gère les mises à jour d'exécution, consultez. the section called “Mises à jour de version de l’environnement d’exécution”

Frameworks Web pris en charge

Vous pouvez utiliser n'importe quel framework Node.js Web qui démarre un serveur HTTP. Les frameworks les plus populaires incluent :

- Express
- Next.js
- Fastify
- Koa

Vous n'avez pas besoin de l'adaptateur Event-to-HTTP AWS Lambda Web Adapter ou d'un autre. Votre application gère les requêtes HTTP directement à l'aide du routage standard et du middleware du framework. Certains frameworks, comme Next.js en mode autonome, lisent leurs propres variables d'environnement pour l'adresse d'écoute. Pour ces frameworks, utilisez un fichier `index.js` d'entrée qui définit ces variables `AWS_LAMBDA_HTTP_ENDPOINT` avant le démarrage du serveur. Pour plus de détails, consultez the section called “Variables d’environnement”. Pour une demande complète, voirthe section called “Minimale Express vigie”.

Node.js modèle d'exécution

Node.jsutilise un modèle d'exécution piloté par les événements. Par défaut, votre JavaScript code Node.js est exécuté sur un seul thread principal et les I/O opérations (appels réseau, accès au

système de fichiers) ne sont pas bloquantes et pilotées par des événements. Votre application peut créer des threads supplémentaires avec le `worker_threads` module si elle en a besoin. Ce modèle a des implications importantes pour les fonctions Web :

Concurrence via asynchrone I/O

Votre serveur gère plusieurs demandes simultanées en utilisant des opérations asynchrones (`async`/`await`, promesses, rappels). Pendant qu'une demande attend une réponse de la base de données, la boucle d'événements répond aux autres demandes. C'est pourquoi les fonctions Web peuvent gérer de nombreuses demandes simultanées dans un seul environnement sans plusieurs threads.

Évitez de bloquer la boucle d'événements

CPU-intensive les opérations synchrones (analyse JSON volumineuse, calculs complexes, lectures de fichiers synchrones) bloquent la boucle d'événements et empêchent le traitement de toutes les autres demandes. Si votre application exécute des CPU-heavy tâches, déchargez-la vers les threads de travail ou réduisez-la `maxConcurrencyPerEnvironment` pour en limiter l'impact.

Demande d'isolation

Comme toutes les demandes partagent le même processus et la même boucle d'événements, évitez de stocker l'état de chaque demande dans des variables globales. Utilisez un contexte intergiciel adapté à la demande (tel que Express`req`/`res`objects) pour isoler les données de demande.

Pour obtenir des conseils sur la configuration en `maxConcurrencyPerEnvironment` fonction des caractéristiques de votre application I/O et du processeur, consultezthe section called “Mise à l’échelle”.

La mémoire et le Node.js tas

Chaque environnement d'exécution dispose de 2 Go de mémoire. Ce qui suit s'applique au Node.js tas V8 :

- Le segment de mémoire par défaut est de 1 024 Mo.
- Pour utiliser un tas plus important, définissez `NODE_OPTIONS` les variables d'environnement de la révision, par exemple `NODE_OPTIONS=--max-old-space-size=1536` (la valeur est en Mo).

- Une valeur que vous définissez `NODE_OPTIONS` remplace la valeur par défaut. Si vous définissez uniquement`--max-old-space-size`, Lambda ne le fait pas et Node.js utilise sa propre valeur par défaut pour cela. `--max-semi-space-size`
- Le tas, les tampons, les allocations natives, le temps d'exécution et les demandes simultanées doivent tous tenir dans les 2 Go de mémoire de l'environnement.

Comment Lambda achemine les demandes vers votre application

Les points de terminaison des fonctions Web acceptent le trafic HTTPS uniquement, sur le port 443. Le protocole HTTP ordinaire n'étant pas diffusé, vous n'avez pas besoin de rediriger le HTTP vers HTTPS ou de configurer le protocole TLS dans votre application.

Lambda met fin au protocole TLS au point de terminaison et transmet chaque requête au serveur HTTP de votre application dans l'environnement d'exécution. Votre application envoie du HTTP simple à l'adresse fournie par Lambda ; vous ne gérez jamais les certificats ou la configuration TLS dans votre code.

Lambda choisit l'hôte et le port sur lesquels votre serveur doit écouter.
Lambda communique l'adresse à votre application par le biais de la variable d'`AWS_LAMBDA_HTTP_ENDPOINT`environnement, au `host:port` format. Utilisez cette variable, définie par Lambda, pour déterminer où votre serveur écoute. Votre application doit lire la variable au démarrage :

```
const [host, port] = (process.env.AWS_LAMBDA_HTTP_ENDPOINT ||
 'localhost:3000').split(':');
app.listen(port, host);
```

Lambda ne définit pas la variable sur votre ordinateur local. L'adresse de secours ne s'applique que lorsque la variable n'est pas définie, elle n'est donc utilisée que dans les exécutions locales. Pour utiliser une adresse locale différente, `AWS_LAMBDA_HTTP_ENDPOINT` configurez-la vous-même. Pour obtenir un exemple, consultez the section called “Exécutez le serveur HTTP localement”.

Lambda ajoute un `lambda-web-request-id` en-tête à chaque demande qu'il transmet à votre application et renvoie la même valeur qu'un en-tête de réponse, afin que vous puissiez corréler une demande client avec les journaux de votre application.

Lambda achemine les requêtes Web vers l'adresse spécifiée par. `AWS_LAMBDA_HTTP_ENDPOINT` Si votre serveur écoute sur un hôte ou un port différent, les demandes ne parviennent pas à votre application.

Votre serveur doit commencer à écouter dans les 10 secondes suivant le démarrage, et chaque demande qu'il traite est liée aux `timeoutSeconds` paramètres de la révision. Pour la séquence de démarrage et d'arrêt, voirthe section called “Cycle de vie environnemental”. Pour savoir comment procéder à la configuration`timeoutSeconds`, consultezthe section called “Révisions”.

Configuration des fonctions Web Lambda

Vous configurez la plupart des paramètres des fonctions Web lors d'une révision, qui est un instantané immuable du code et de la configuration de votre application. Comme une révision est immuable, la modification d'un paramètre de révision implique la création d'une nouvelle révision avec les valeurs mises à jour. Vous définissez les balises et la politique basée sur les ressources dans la fonction Web. Ses révisions et ses points de terminaison héritent de ses balises, et la politique basée sur les ressources contrôle qui peut agir sur la fonction Web, ses révisions et ses points de terminaison. Les paramètres du point de terminaison s'appliquent à chaque point de terminaison, notamment le type d'authentification, le mode de déploiement automatique, les pondérations de révision, le dimensionnement et la régulation. Vous pouvez les modifier sans créer de nouvelle révision. Les rubriques suivantes décrivent les paramètres que vous pouvez configurer.

Rubriques

- Package de déploiement de fonctions Web
- Architecture de l’ensemble des instructions
- Délai d'expiration de la demande
- Variables d’environnement
- Fonctions Web de balisage
- Utilisation du point de terminaison des métadonnées

Package de déploiement de fonctions Web

Vous empaquetez votre code de fonction Web sous forme de fichier .zip et vous le stockez dans un compartiment Amazon S3 versionné. La révision fait `codeConfig` référence au compartiment, à la clé et éventuellement à une version d'objet. Si vous omettez la version, Lambda utilise la dernière

version au moment de la création, de sorte que chaque révision pointe vers une version spécifique de votre package. Le téléchargement d'un nouveau package avec la même clé ne modifie pas les révisions existantes, et vous pouvez revenir à une version antérieure tant que la version de l'objet reste dans le compartiment.

Le package doit inclure le fichier d'entrée de votre application et toutes ses dépendances (par exemple,`node_modules`). Par défaut, Lambda charge `index.js` à la racine du package en tant que fichier d'entrée et l'exécute pour démarrer votre serveur HTTP. Pour utiliser un nom ou un chemin différent (par exemple,`dist/index.js`), définissez la variable d'`AWS_LAMBDA_NODEJS_ENTRYPOINT`environnement ; voirthe section called “Variables d’environnement”.

Pour savoir comment créer et télécharger le package sur Amazon S3 et créer une révision qui le référence, consultez the section called “Code dans Amazon S3” etthe section called “Créez votre première fonction Web”.

Architecture de l’ensemble des instructions

Les fonctions Web fonctionnent exclusivement sur l'architecture Arm64, alimentée par des processeurs AWS Graviton. Contrairement à Lambda Event Functions, vous ne pouvez pas choisir le jeu d'instructions : il n'y a aucun paramètre d'architecture à configurer.

Chaque environnement d'exécution de fonction Web utilise 2 vCPU Arm64. Un quota par région limite la capacité du vCPU Arm64 de votre compte. Pour ce quota, consultez the section called “Fonctions Web Lambda”. Pour les statistiques d'utilisation qui montrent votre consommation par rapport à celle-ci, voirthe section called “Indicateurs régionaux d'utilisation et de limitation”.

Créez des dépendances natives pour Linux sur arm64 (aarch64). Le JavaScript code pur Node.js n'a pas besoin d'être modifié. Toute dépendance avec des binaires natifs doit fournir une version Linux arm64. Construisez la dépendance sur une machine Linux arm64 ou dans un conteneur Linux arm64, ou compilez-la de manière croisée pour Linux arm64. Pour un exemple d'installation de dépendances dans un conteneur Arm64, consultez. the section called “Testez le package de déploiement”

Délai d'expiration de la demande

Le `timeoutSeconds` paramètre contrôle la durée maximale pendant laquelle une seule requête HTTP peut être exécutée avant que Lambda ne l'arrête. Les valeurs valides sont comprises entre 3 et 900 secondes (15 minutes). Le durée par défaut est 30 secondes.

Choisissez une valeur de délai d'attente en fonction de la demande la plus longue attendue de votre application. Si le délai d'expiration est trop faible, les demandes de longue durée échouent. Une valeur trop élevée permet aux requêtes bloquées de s'exécuter plus longtemps avant que Lambda ne les arrête.

Lorsqu'une requête autre que le streaming dépasse le délai imparti, Lambda renvoie HTTP 504 avec un en-tête de. `lambda-web-error-type` `Runtime.RequestTimeout` Pour une réponse en streaming, le délai limite l'ensemble du flux. Lorsque le délai est écoulé, Lambda met fin au flux et le client reçoit le code d'état déjà envoyé, généralement 200, avec un corps tronqué et sans en-tête. `lambda-web-error-type`

Variables d’environnement

Les variables d'environnement sont des paires clé-valeur accessibles au code de votre application au moment de l'exécution. Utilisez des variables d'environnement pour les configurations non sensibles que vous souhaitez modifier sans modifier le code, telles que les indicateurs de fonctionnalité, les niveaux de journalisation et les identifiants de ressources tels que le nom d'hôte d'une base de données. Pour les valeurs sensibles telles que les clés d'API et les informations d'identification de base de données, ne les stockez pas dans des variables d'environnement. Utilisez plutôt Secrets Manager ou AWS Systems Manager Parameter Store et récupérez les valeurs lors de l'exécution.

Les variables d'environnement sont définies lorsque vous créez la révision et sont immuables après la création. Pour modifier une variable d'environnement, créez une nouvelle révision. Dans la nouvelle version, spécifiez toutes les variables d'environnement et tous les `serviceConfig` paramètres que vous souhaitez conserver, et pas uniquement les valeurs qui changent. Les paramètres que vous omettez prennent leurs valeurs par défaut, et les variables d'environnement que vous omettez ne sont pas définies.

Lambda définit la variable d'environnement suivante spécifiquement pour les fonctions Web :

- **`AWS_LAMBDA_HTTP_ENDPOINT`**— L'hôte et le port sur lesquels votre serveur HTTP doit écouter, au `host:port` format. Lambda définit cette variable et achemine les demandes vers cette adresse. Lisez-le dans le code de votre application et liez exactement cet hôte et ce port. Vous ne pouvez pas définir cette variable dans les variables d'environnement d'une révision. Liez toujours à l'adresse de cette variable, et non `localhost` à un port codé en dur. Le moteur d'exécution attend que votre serveur accepte une connexion à cette adresse, et l'initialisation échoue si ce n'est jamais le cas. Utilisez une adresse de secours uniquement pour les exécutions locales. Dans une fonction Web, Lambda définit toujours cette variable.

Les fonctions Web reçoivent également d'autres variables d'environnement d'exécution Lambda, telles que `AWS_LAMBDA_FUNCTION_MEMORY_SIZEAWS_LAMBDA_METADATA_API`, et. `AWS_LAMBDA_METADATA_TOKEN` Pour la liste générale, voirVariables d'environnement d'exécution définies. Si votre code ou une bibliothèque lit une variable de cette liste, vérifiez que Lambda la définit dans une fonction Web avant de vous y fier. Les fonctions Web ne reçoivent pas toutes les variables de cette liste.

Les noms de variables d'environnement suivants sont réservés aux fonctions Web Lambda et ne peuvent pas être définis. Si vous en spécifiez une, Lambda rejette la demande de création d'une fonction Web ou d'une révision :

- `AWS_ACCESS_KEY`, `AWS_ACCESS_KEY_ID`, `AWS_SECRET_ACCESS_KEY`, `AWS_SECRET_KEY`, `AWS_SECURITY_TOKEN`, et `AWS_SESSION_TOKEN`
- `AWS_DEFAULT_REGION` et `AWS_REGION`
- `AWS_LAMBDA_HTTP_ENDPOINT`, `AWS_LAMBDA_RUNTIME_API`, `AWS_LAMBDA_INITIALIZATION_TYPE`, et `AWS_LAMBDA_FUNCTION_MEMORY_SIZE`
- `AWS_LAMBDA_METADATA_API` et `AWS_LAMBDA_METADATA_TOKEN`

Certains frameworks lisent plutôt leurs propres variables d'environnement pour l'adresse d'écoute. Par exemple, le mode Next.js autonome lit `HOSTNAME` et. `PORT` Pour de tels frameworks, utilisez un fichier `index.js` d'entrée qui définit ces variables `AWS_LAMBDA_HTTP_ENDPOINT` avant de démarrer le serveur.

Par défaut, le moteur d'exécution se charge `index.js` à la racine de votre package de déploiement en tant que fichier d'entrée de votre application. Le moteur d'exécution ne lit pas le point d'entrée depuis`package.json`. Si votre fichier d'entrée a un nom ou un chemin différent (par exemple,`dist/index.js`), définissez la variable d'`AWS_LAMBDA_NODEJS_ENTRYPOINT`environnement sur son chemin, par rapport à la racine de votre package.

L'exemple suivant montre comment lire la variable d'`AWS_LAMBDA_HTTP_ENDPOINT`environnement dans une Node.js application :

```
// Lambda provides the address to bind in AWS_LAMBDA_HTTP_ENDPOINT ("host:port").
// The fallback applies only when running locally.
const [host, port] = (process.env.AWS_LAMBDA_HTTP_ENDPOINT ||
 'localhost:3000').split(':');
app.listen(port, host, () => {
  console.log(`Server listening on ${host}:${port}`);
```

```
});
```

Pour définir vos propres variables d'environnement, ajoutez une `environmentVariables` carte à l'`serviceConfig`objet lorsque vous créez une révision, comme dans l'exemple suivant. Pour la commande complète, voirthe section called “Création d'une révision”.

```
{
  "executionRoleArn": "arn:aws:iam::111122223333:role/my-web-function-role",
  "environmentVariables": {
    "DATABASE_URL": "my-database-endpoint",
    "LOG_LEVEL": "info",
    "FEATURE_FLAG_NEW_UI": "true"
  }
}
```

Si vous spécifiez une clé gérée par le client, Lambda chiffre les variables d'environnement au repos avec cette clé. Pour plus d'informations, consultez the section called “Chiffrement au repos”.

Fonctions Web de balisage

Les balises sont des libellés à valeur clé que vous associez à une fonction Web pour organiser vos ressources et contrôler l'accès. Les balises s'appliquent à la ressource Web Function.

Pour ajouter des balises lorsque vous créez une fonction Web, utilisez le `tags` paramètre de`CreateWebFunction`. Pour ajouter, supprimer ou répertorier des balises ultérieurement, utilisez les `TagResource` `ListTags` opérations`UntagResource`, et.

Vous pouvez utiliser les balises de différentes manières :

- Organisation et recherche : regroupez et recherchez les fonctions Web par attributs tels que le projet, l'environnement ou l'équipe. Vous pouvez trouver une fonction Web par ses balises uniquement dans sa région d'origine. Pour plus d’informations, consultez the section called “Visibilité des répliques”.
- Attribute-based contrôle d'accès (ABAC) — Écrivez des politiques Gestion des identités et des accès AWS (IAM) qui autorisent ou refusent des actions basées sur des balises. `aws:ResourceTag/${TagKey}`À utiliser pour les actions sur une fonction Web, ses révisions et ses points de terminaison, qui héritent des balises de la fonction Web. `CreateWebFunction`Activé, vous pouvez également utiliser `aws:RequestTag/${TagKey}` et`aws:TagKeys`. Vous ne pouvez pas étiqueter directement les révisions ou les points de

terminaison. Pour plus d'informations, consultez the section called "Permissions" et the section called "Contrôle d'accès".

Les balises possèdent les exigences suivantes :

- Les clés de balise comportent de 1 à 128 caractères.
- Les valeurs des balises sont comprises entre 0 et 256 caractères.
- Les clés et les valeurs peuvent contenir des lettres, des chiffres, des espaces et des caractères `_ . : / = + - @`.

Utilisation du point de terminaison des métadonnées

Le point de terminaison des métadonnées Lambda est une API HTTP locale au sein de l'environnement d'exécution. Il renvoie les métadonnées dans un format JSON simple, y compris l'ID de la zone de disponibilité (AZ) dans laquelle l'environnement est exécuté. Utilisez-le pour acheminer vers des ressources de même zone, telles qu'Amazon et ElastiCache Amazon RDS, afin de réduire le temps de latence. Vous pouvez également l'utiliser pour implémenter des modèles de AZ-aware résilience.

> **Note**
>
> Une fonction Web exécute un serveur Web permanent plutôt qu'un gestionnaire par appel. Lisez le point de terminaison des métadonnées une fois au démarrage de l'application et mettez la valeur en cache, ou lisez-le par demande si vous en avez besoin dans le contexte de la demande. Ne supposez pas qu'il existe un nouveau gestionnaire par appel. Pour une fonction Web multirégionale, le point de terminaison indique l'AZ Région AWS qui répond à la demande.

Sections

- Prise en main

Prise en main

Powertools for AWS Lambda fournit un utilitaire permettant d'accéder au point de terminaison des métadonnées Lambda. L'utilitaire met en cache la réponse après le premier appel. Pour plus

d'informations, consultez la section Métadonnées dans la documentation de Powertools for AWS Lambda TypeScript ().

Les fonctions Web étant exécutées surNode.js, l'exemple suivant utilise l'utilitaire de métadonnées Powertools for AWS Lambda pour lire l'ID AZ une fois au démarrage du serveur et le mettre en cache pendant toute la durée du processus. Exécutez la commande npm suivante pour installer le package Powertools et Express :

```
npm install @aws-lambda-powertools/commons express
```

L'exemple suivant l'utilise à des Express fins d'illustration. La même approche fonctionne avec n'importe quel framework Node.js Web ; voirthe section called “Frameworks Web pris en charge”. Lisez l'ID AZ au démarrage et réutilisez la valeur mise en cache lors du traitement des demandes :

Example Récupération de l'identifiant AZ avec Powertools au démarrage () TypeScript

```
import express from 'express';
import { getMetadata } from '@aws-lambda-powertools/commons/utils/metadata';

const app = express();

// Read the AZ ID once at startup and cache it for the life of the server.
const { AvailabilityZoneID: azId } = await getMetadata();

// Lambda provides the address to bind in AWS_LAMBDA_HTTP_ENDPOINT ("host:port").
// The fallback applies only when running locally.
const [host, port] = (process.env.AWS_LAMBDA_HTTP_ENDPOINT ||
 'localhost:3000').split(':');

app.get('/', (req, res) => {
  res.json({ azId });
});

app.listen(port, host, () => {
  console.log(`Server listening on ${host}:${port}, AZ: ${azId}`);
});
```

Vous pouvez également appeler directement le point de terminaison des métadonnées. Lambda définit automatiquement les variables d'`AWS_LAMBDA_METADATA_TOKEN`environnement `AWS_LAMBDA_METADATA_API` et dans chaque environnement d'exécution, et vous incluez le jeton avec le schéma Bearer dans l'en-tête. `Authorization` Pour l'URL du point de terminaison, les

formats de demande et de réponse, ainsi que les réponses aux erreurs, consultezthe section called “Point final de métadonnées”.

Par exemple, lisez l'adresse du serveur de métadonnées depuis `AWS_LAMBDA_METADATA_API` et envoyez une requête GET authentifiée :

```
METADATA_ENDPOINT="http://${AWS_LAMBDA_METADATA_API}/2026-01-15/metadata/execution-
environment"
RESPONSE=$(curl -s -H "Authorization: Bearer ${AWS_LAMBDA_METADATA_TOKEN}"
 "$METADATA_ENDPOINT")
AZ_ID=$(echo "$RESPONSE" | jq -r '.AvailabilityZoneID')
```

Le point de terminaison revient`application/json`. Par exemple : `{"AvailabilityZoneID": "use1-az1"}`.

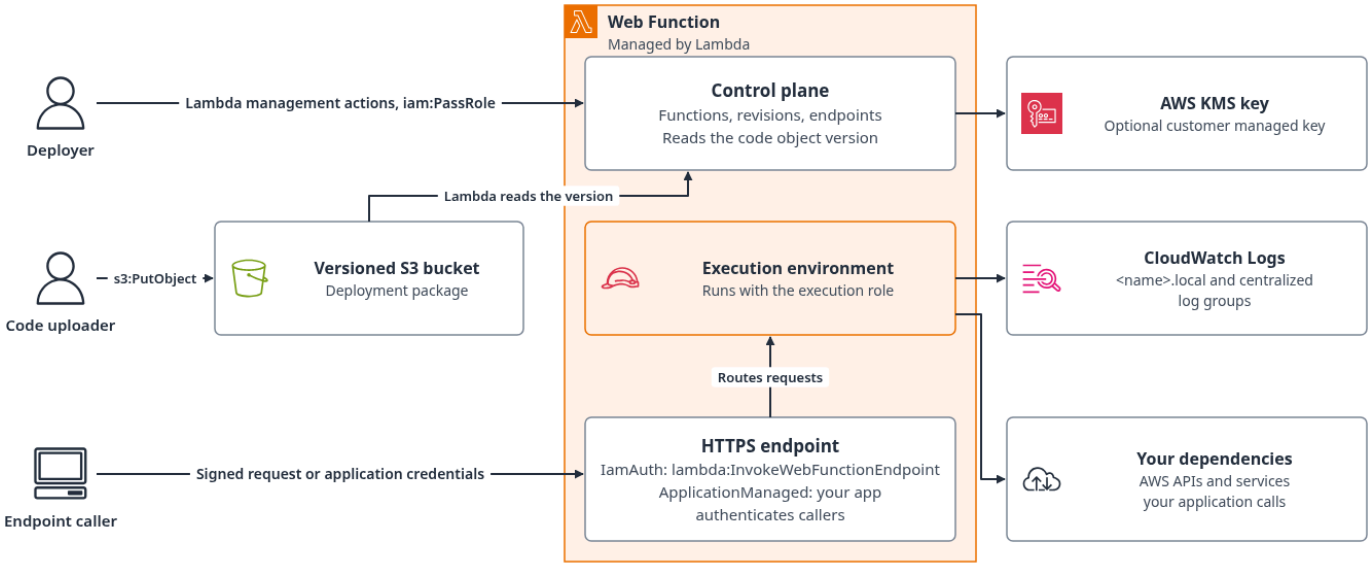
Autorisations relatives à la fonction Web Lambda

Les fonctions Web Lambda utilisent Gestion des identités et des accès AWS (IAM) pour contrôler ce que le code de votre application peut faire (le rôle d'exécution) et qui peut accéder à votre fonction Web (politiques basées sur les ressources). Cette page explique comment configurer chaque type.

- Rôle d'exécution : rôle IAM assumé par votre code de fonction Web pour accéder à AWS des services tels qu'Amazon CloudWatch Logs, DynamoDB ou Amazon S3.
- Resource-based politiques : politique attachée à votre fonction Web. Il définit quels principaux ou AWS services IAM peuvent effectuer des actions de fonction Web, telles que l'appel d'un point de terminaison dont le type d'authentification est`IamAuth`, ce qui signifie que Lambda authentifie les demandes auprès d'IAM. Pour plus d’informations, consultez the section called “Type d’authentification”. Le principal IAM d'un autre compte a également besoin d'une autorisation basée sur l'identité.

Le schéma suivant montre les identités qui nécessitent des autorisations et ce que chacune d'elles utilise. Le déployeur appelle les actions et les `iam:PassRole` besoins de gestion Lambda sur le rôle d'exécution. Le téléchargeur de code doit `s3:PutObject` se trouver sur le compartiment Amazon S3 versionné, et Lambda lit la version de l'objet de code. Lambda peut chiffrer le code de votre fonction Web et vos variables d'environnement à l'aide d'une clé optionnelle gérée par le client. AWS KMS Votre code s'exécute avec le rôle d'exécution, qui donne accès à Amazon CloudWatch Logs et à vos dépendances. L'appelant a besoin `lambda:InvokeWebFunctionEndpoint` d'un point de

`IamAuth` terminaison ou d'informations d'identification d'application pour un `ApplicationManaged` point de terminaison.



Grant each actor only what its role needs. With IamAuth, endpoint access can also come from a resource-based policy.

Rôle d'exécution

Le rôle d'exécution est un rôle IAM que Lambda assume lorsqu'il exécute le code de votre fonction Web. Votre application utilise les autorisations de ce rôle pour interagir avec d'autres AWS services. Au minimum, votre fonction Web doit être autorisée à écrire des CloudWatch journaux sur Amazon Logs afin que vous puissiez surveiller votre application. Si votre application lit depuis DynamoDB, écrit sur Amazon S3 ou appelle AWS d'autres services, vous ajoutez ces autorisations au rôle d'exécution.

Création d'un rôle d'exécution

Pour créer un rôle d'exécution pour votre fonction Web, créez un rôle IAM avec une politique de confiance qui permet au principal du service Lambda de l'assumer, et associez une politique d'autorisation qui accorde l'accès dont votre application a besoin.

Pour créer un rôle d'exécution (AWS CLI)

1. Créez un fichier nommé `trust-policy.json` avec la politique de confiance suivante. Cette politique permet au directeur du service Lambda d'assumer le rôle en votre nom.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "lambda.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

2. Créez le rôle.

```
aws iam create-role \
    --role-name my-web-function-role \
    --assume-role-policy-document file://trust-policy.json
```

3. Attachez la politique de gestion des rôles d'exécution de AWS Lambda base. Cette politique accorde des autorisations pour créer des groupes de journaux, des flux de journaux et écrire des événements de journal sur Amazon CloudWatch Logs.

```
aws iam attach-role-policy \
    --role-name my-web-function-role \
    --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole
```

Si vous préférez créer une politique d'autorisations personnalisée au lieu d'utiliser la politique gérée, les autorisations minimales dont votre fonction Web a besoin pour se connecter sont les suivantes :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource": [
```

```
                "arn:aws:logs:us-east-1:111122223333:log-group:/aws/lambda/web/my-web-
app:*",
                "arn:aws:logs:*:111122223333:log-group:/aws/lambda/web/my-web-
app.local:*"
            ]
        }
    ]
}
```

La politique couvre deux groupes de journaux. Lambda écrit les journaux régionaux dans le `.local` groupe de journaux, puis les centralise dans le groupe de journaux sans le suffixe dans la région d'origine. L'ARN du groupe de journaux centralisé utilise la région d'origine. L'`.local`ARN utilise un caractère générique de région car Lambda écrit dans ce groupe dans chaque région où un point de terminaison dessert du trafic. Cela permet à un rôle d'exécution de prendre en charge des points de terminaison dotés de différents ensembles de régions. Si le rôle ne peut pas écrire dans le groupe de `.local` journaux d'une région, Lambda ne fournit pas les journaux de cette région. Si vous utilisez un groupe de journaux personnalisé, remplacez les deux ARN par le nom de votre groupe de journaux et le nom de votre groupe de journaux suivis `.local` de. Pour plus d'informations, consultez the section called “Groupes de journaux”.

Ajouter des autorisations pour d'autres services

Si votre application accède à d'autres AWS services, ajoutez les autorisations correspondantes au rôle d'exécution. L'exemple suivant ajoute un accès en lecture à une table DynamoDB et un accès en écriture à un compartiment Amazon S3.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:us-east-1:111122223333:log-group:/aws/lambda/web/my-web-
app:*",
                "arn:aws:logs:*:111122223333:log-group:/aws/lambda/web/my-web-
app.local:*"
```

```
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "dynamodb:GetItem",
                "dynamodb:Query"
            ],
            "Resource": "arn:aws:dynamodb:us-east-1:111122223333:table/my-table"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::my-output-bucket/*"
        }
    ]
}
```

L'identité IAM qui crée une fonction Web ou une révision utilise ses propres autorisations, et non le rôle d'exécution. Cette identité nécessite `lambda:CreateWebFunction` ou`lambda:CreateWebFunctionRevision`, `iam:PassRole` sur le rôle d'exécution, un accès en lecture au package de déploiement dans Amazon S3. Pour les autorisations Amazon S3, consultezthe section called “Autorisations de l'appelant”. Si vous utilisez une clé gérée par le client pour chiffrer le code de votre fonction Web et les variables d'environnement, cette identité nécessite également AWS KMS des autorisations. Pour plus d’informations, consultez the section called “Chiffrement au repos”.

Resource-based politiques

Une politique basée sur les ressources est un document de politique JSON que vous attachez à votre fonction Web. Il peut accorder n'importe quelle action de fonction Web `lambda:CreateWebFunction` à l'exception des principaux ou AWS des services IAM. Par exemple, il peut accorder une autorisation `lambda:InvokeWebFunctionEndpoint` pour un `IamAuth` point de terminaison. Il peut également accorder des actions de gestion telles que `lambda:GetWebFunctionlambda:CreateWebFunctionRevision`, et`lambda:UpdateWebFunctionEndpoint`.

La pièce jointe à la politique et ses déclarations utilisent différents ARN de ressources :

- ARN de la fonction Web : utilisez cet ARN avec `PutResourcePolicy` `GetResourcePolicyDeleteResourcePolicy`, et, et dans l'`Resource`élément d'une instruction qui autorise une action sur la fonction Web elle-même, tel que `lambda:GetWebFunction`lambda:CreateWebFunctionRevision, oulambda:CreateWebFunctionEndpoint. Par exemple : `arn:aws:lambda:us-east-1:111122223333:web-function/my-function`. Pour une action sur un point de terminaison existant, par exemple`lambda:UpdateWebFunctionEndpoint`, utilisez l'ARN du point de terminaison. Pour une action sur une révision existante, par exemple`lambda:DeleteWebFunctionRevision`, utilisez l'ARN de révision. Pour couvrir tous les points de terminaison de la fonction Web, utilisez`arn:aws:lambda:us-east-1:111122223333:web-function/my-function/endpoint/*`.
- ARN du point de terminaison — Utilisez cet ARN dans l'`Resource`élément d'une déclaration de politique qui accorde`lambda:InvokeWebFunctionEndpoint`. Par exemple : `arn:aws:lambda:us-east-1:111122223333:web-function/my-function/endpoint/prod`.

Pour un principal IAM du même compte, la politique basée sur l'identité du principal ou la politique basée sur les ressources de la fonction Web peuvent accorder l'autorisation. Pour un directeur IAM d'un autre compte, les deux politiques doivent accorder une autorisation. Cela s'applique à la fois aux actions d'appel et aux actions de gestion.

Pour autoriser ou refuser des actions basées sur les balises d'une fonction Web, utilisez le contrôle d'accès basé sur les attributs (ABAC). Pour connaître les clés de condition prises en charge, consultezthe section called “Étiquettes”.

> **Note**
>
> Les fonctions Web ne sont pas `AddPermission` compatibles avec`RemovePermission`, ou`GetPolicy`. Gérez la politique avec `PutResourcePolicy`GetResourcePolicy, et`DeleteResourcePolicy`.

Utilisez des politiques basées sur les ressources lorsque :

- Vous souhaitez accorder l'accès Invoke à un principal dans le cadre d'une autre procédure Compte AWS (invocation entre comptes).
- Vous souhaitez accorder l'accès Invoke à un AWS service tel que CloudFront.

- Vous souhaitez laisser un directeur d'un autre administrateur Compte AWS gérer la fonction Web, par exemple pour créer des révisions ou mettre à jour des points de terminaison.
- Pour l'invocation d'un même compte, vous ne pouvez pas modifier la politique IAM de l'appelant (par exemple, lorsque l'appelant est géré par une autre équipe).

Les politiques publiques ne sont pas autorisées

Vous ne pouvez pas associer une politique basée sur les ressources publiques à une fonction Web. Si une politique est publique, la demande échoue avec un`ValidationException`.

Dans cette section, public décrit une politique qui accorde l'accès à un ensemble non spécifié de principes. Il ne décrit pas l'accessibilité du réseau ou le type d'authentification du point de terminaison.

Qu'est-ce qui rend une politique publique

Une politique est publique à moins qu'elle ne limite les personnes autorisées à appeler la ressource à un ensemble bien défini de principes. Lambda part du principe que la politique est publique, puis évalue si elle est considérée comme non publique. Une politique est publique si elle autorise un principal que n'importe quel AWS client peut assumer. Le cas le plus courant est celui d'un joker principal non restreint, comme dans l'exemple suivant. Lambda rejette cette politique avec un. `ValidationException` Ne l'utilisez pas.

```
{
  "Effect": "Allow",
  "Principal": "*",
  "Action": "lambda:InvokeWebFunctionEndpoint",
  "Resource": "arn:aws:lambda:us-west-2:123456789012:web-function/my-web-function/
endpoint/prod"
}
```

Les restrictions suivantes ne rendent pas une politique non publique :

- Conditions relatives à l'adresse IP. Il ne suffit pas `aws:SourceIp` de se limiter à une plage CIDR.
- Principaux fédérés. Un `Principal` bloc qui nomme un fournisseur d'identité fédéré ne limite pas l'accès à un ensemble d'identités bien défini.
- Clés de condition qui décrivent la ressource. Les clés telles que le type d'authentification du point de terminaison décrivent comment la ressource est configurée, et non qui appelle, de sorte qu'elles ne peuvent pas restreindre le principal.

Il existe deux manières de rendre une politique non publique.

Spécifiez les principes dans le bloc Principal

Énumérez un ou plusieurs principes entièrement spécifiés dans le `Principal` bloc. Les valeurs ne doivent pas contenir de caractères génériques ni de variables de politique. Le nombre de directeurs n'a pas d'importance.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "123456789012",
      "111122223333"
    ]
  },
  "Action": "lambda:InvokeWebFunctionEndpoint",
  "Resource": "arn:aws:lambda:us-west-2:123456789012:web-function/my-web-function/
endpoint/prod"
}
```

Un principal IAM d'un autre compte a également besoin d'une autorisation basée sur l'identité pour appeler le point de terminaison.

Utiliser une clé de condition fiable

Limitez l'une des clés de condition suivantes à une valeur fixe. Ces clés identifient l'appelant authentifié et ne peuvent pas être définies par le demandeur.

- `aws:PrincipalAccount`
- `aws:PrincipalArn`
- `aws:PrincipalOrgID`
- `aws:PrincipalOrgPaths`
- `aws:SourceAccount`
- `aws:SourceArn`
- `aws:SourceOrgID`
- `aws:SourceOrgPaths`
- `aws:SourceVpc`

- `aws:SourceVpcArn`
- `aws:SourceVpce`
- `aws:VpceAccount`
- `aws:VpceOrgID`
- `aws:VpceOrgPaths`
- `aws:Ec2InstanceSourceVpc`
- `aws:UserId`
- `aws:PrincipalServiceName`
- `aws:PrincipalServiceNamesList`
- `aws:PrincipalIsAWSService`
- `lambda:SourceFunctionArn`

Le fait de nommer une clé fiable ne suffit pas à lui seul. Vous devez également restreindre la valeur :

- Les valeurs de chaîne ne doivent pas contenir de caractères génériques ni de variables de politique.
- Les valeurs ARN ne doivent pas contenir de caractères génériques ou de variables de politique dans les cinq premiers champs de l'ARN : `arn` partition, service, région et ID de compte. Les caractères génériques sont autorisés dans la partie ressource.
- `aws:PrincipalIsAWSService` doit être défini sur `true`.

La politique suivante accorde aux responsables de votre organisation l'autorisation basée sur les ressources requise pour appeler le point de terminaison et n'est pas considérée comme publique. Le principal IAM d'un autre compte a également besoin d'une autorisation basée sur l'identité.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowOrgAccess",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "lambda:InvokeWebFunctionEndpoint",
```

```
      "Resource": "arn:aws:lambda:us-west-2:123456789012:web-function/my-web-function/
endpoint/prod",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalOrgID": "o-a1b2c3d4e5"
        }
      }
    }
  ]
}
```

Cross-account accès

La politique basée sur les ressources suivante accorde à un rôle IAM spécifique dans un autre compte l'autorisation d'invoquer un point de terminaison de votre fonction Web. Le rôle a également besoin d'une autorisation basée sur l'identité pour appeler le point de terminaison.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCrossAccountInvoke",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::444455556666:role/caller-role"
            },
            "Action": "lambda:InvokeWebFunctionEndpoint",
            "Resource": "arn:aws:lambda:us-east-1:111122223333:web-function/my-
function/endpoint/prod"
        }
    ]
}
```

Pour que l'invocation entre comptes réussisse, toutes les conditions suivantes doivent être remplies :

- La politique basée sur l'identité de l'appelant accorde une `lambda:InvokeWebFunctionEndpoint` autorisation sur l'ARN du point de terminaison.
- La politique basée sur les ressources de la fonction Web accorde l'autorisation à l'appelant (comme indiqué ci-dessus).
- Le point de terminaison utilise `IamAuth` l'authentification afin que Lambda évalue les informations d'identification de l'appelant.

Accorder l'accès à un AWS web

La politique basée sur les ressources suivante accorde au principal du CloudFront service l'autorisation d'appeler votre fonction Web. Utilisez cette politique lorsque vous configurez une CloudFront distribution avec le point de terminaison de votre fonction Web comme origine.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCloudFrontInvoke",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudfront.amazonaws.com"
            },
            "Action": "lambda:InvokeWebFunctionEndpoint",
            "Resource": "arn:aws:lambda:us-east-1:111122223333:web-function/my-
function/endpoint/prod",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn":
 "arn:aws:cloudfront::111122223333:distribution/EDFDVBD6EXAMPLE"
                }
            }
        }
    ]
}
```

La `aws:SourceArn` condition restreint l'accès à une CloudFront distribution spécifique. Sans cette condition, toute CloudFront distribution dans n'importe quel compte pourrait invoquer votre fonction Web.

Réplication et cohérence éventuelle

Lorsque vous attachez ou mettez à jour une politique basée sur les ressources à une fonction Web qui possède MultiRegionou des points de PerRegionterminaison, Lambda réplique la politique sur toutes les répliques sur lesquelles les points de terminaison opèrent. Régions AWS Cette réplication est finalement cohérente.

Pendant la fenêtre de réplication, Lambda peut évaluer les demandes dans les régions de réplication par rapport à la version précédente de la politique. Autrement dit :

- Il est possible qu'une autorisation nouvellement ajoutée ne prenne pas effet immédiatement dans toutes les régions.
- Lambda peut toujours respecter une autorisation récemment supprimée dans certaines régions jusqu'à ce que la réplication soit terminée.

Il n'existe aucun signal d'achèvement visible par le client pour la réplication des politiques. Testez le comportement d'autorisation ou de refus attendu dans chaque région du point de terminaison avant de vous fier à la nouvelle politique. Pour le confinement d'urgence, mettez à jour le routage du trafic ou configurez le point de terminaison de manière `throttleConfig.rateLimit` `0` à ce qu'il bloque tout le trafic pendant que le changement de politique se propage. Pour plus d'informations, consultez the section called “Étranglement”.

Pour les HomeRegionterminaux, la politique s'applique uniquement dans la région d'origine et ne nécessite pas de réplication entre régions. Un changement peut tout de même prendre un peu de temps pour prendre effet.

Autorisations pour configurer le réseau

L'identité qui configure le réseau doit être autorisée à créer ou à mettre à jour les ressources Lambda pertinentes. Il a également besoin d'une autorisation pour transmettre les rôles et le connecteur requis. En fonction de l'opération, les autorisations incluent :

- `lambda:CreateNetworkConnector`
- `lambda:UpdateNetworkConnector`
- `lambda:GetNetworkConnector`
- `lambda:CreateWebFunction`
- `lambda:CreateWebFunctionRevision`
- `lambda:UpdateWebFunctionEndpoint`
- `lambda:PassNetworkConnector`
- `iam:PassRole`

L'appelant doit être connecté `lambda:PassNetworkConnector` au connecteur référencé chaque fois qu'un `create-web-function-revision` appel `create-web-function` ou est défini. `egressNetworkConnectorArn` Élargissez cette autorisation aux ressources de connecteur approuvées. `iam:PassRole`Portez sur les rôles d'exécution approuvés, que vous transmettez

lorsque vous créez une fonction Web ou une révision, et sur les rôles d'opérateur approuvés, que vous transmettez lorsque vous créez ou mettez à jour un connecteur réseau. Pour la politique d'autorisations relatives au rôle d'opérateur, voirthe section called “Autorisations relatives au rôle d'opérateur”.

Contrôle d'accès aux terminaux Lambda Web Function

Vous pouvez contrôler l'accès aux points de terminaison de vos fonctions AWS Lambda Web à l'aide de ceux `AuthType` que vous avez définis sur chaque point de terminaison. Selon le type d'authentification, vous pouvez également associer une politique basée sur les ressources à la fonction Web pour contrôler qui peut invoquer un point de terminaison.

Lorsque vous configurez un point de terminaison, vous spécifiez l'une des `AuthType` options suivantes :

`IamAuth`

Avec ce type d'authentification, Lambda utilise Gestion des identités et des accès AWS (IAM) pour authentifier et autoriser les demandes en fonction de la politique d'identité de l'appelant et de la politique basée sur les ressources de la fonction Web. Soit l'appelant signe les demandes directement avec AWS Signature Version 4 (SigV4), soit avec Signature Version 4a (SigV4a) pour les `MultiRegion` terminaux, soit Amazon CloudFront signe Service AWS en son nom lorsqu'il fait face au terminal (voir). the section called “CloudFront intégration” Choisissez cette option lorsque vous souhaitez que Lambda applique le contrôle d' IAM-based accès à votre terminal.

`ApplicationManaged`

Lambda n'authentifie ni n'autorise les demandes. Chaque demande atteint votre fonction, et votre code de fonction est responsable de toute authentification. Choisissez cette option pour les points de terminaison publics ou lorsque vous gérez l'authentification dans votre propre code.

L'action IAM pour appeler un point de terminaison est. `lambda:InvokeWebFunctionEndpoint`

Vous définissez le type d'authentification d'un point de terminaison avec le `--auth-type` paramètre lorsque vous créez le point de terminaison (`create-web-function-endpoint`), et vous pouvez le modifier ultérieurement avec`update-web-function-endpoint`. Pour la commande de création, voirthe section called “Création d’un point de terminaison”. Pour les propriétés que vous pouvez modifier, consultezthe section called “Mise à jour d'un terminal”.

Utilisation du type **`IamAuth`**d'authentification

Si vous choisissez le type `IamAuth` d'authentification, les appelants doivent signer chaque demande avec SigV4 (SigV4a pour les `MultiRegion` points de terminaison) et doivent être autorisés à invoquer le point de terminaison. En fonction de l'auteur de la demande, vous accordez cette autorisation avec une politique basée sur les ressources sur la fonction Web, une politique basée sur l'identité de l'appelant, ou les deux.

Si l'appelant se trouve dans la même zone Compte AWS que la fonction Web, ils peuvent être accordés `lambda:InvokeWebFunctionEndpoint` par le biais d'une politique basée sur l'identité ou de la politique basée sur les ressources de la fonction. Si l'appelant utilise un autre compte, il a besoin à la fois d'une politique basée sur l'identité autorisant l'action et d'une politique basée sur les ressources concernant la fonction qui l'autorise.

Resource-based les politiques sont associées à la fonction Web, mais chaque instruction peut les étendre `Resource` à un ARN de point de terminaison spécifique. La politique basée sur les ressources suivante permet au `InvokeRole` rôle du compte d'invoquer le point `222233334444` de `prod` terminaison de : `my-function`

Example Cross-account politique basée sur les ressources

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::222233334444:role/InvokeRole"
            },
            "Action": "lambda:InvokeWebFunctionEndpoint",
            "Resource": "arn:aws:lambda:us-east-1:111122223333:web-function/my-
function/endpoint/prod"
        }
    ]
}
```

Pour associer la politique basée sur les ressources, utilisez `put-resource-policy` la fonction ARN (et non un ARN de point de terminaison) :

```
aws lambda-web put-resource-policy \
```

```
    --resource-arn "arn:aws:lambda:us-east-1:111122223333:web-function/my-function" \
    --policy file://policy.json \
    --region us-east-1
```

Vous pouvez consulter ou supprimer la politique à l'aide de `get-resource-policy` et`delete-resource-policy`.

Une fonction Web possède une politique basée sur les ressources et la `put-resource-policy` remplace. Pour ajouter une instruction, telle que l' CloudFront instruction inthe section called “CloudFront intégration”, obtenez la politique actuelle avec`get-resource-policy`, ajoutez l'instruction à son `Statement` tableau et transmettez la valeur renvoyée `revisionId` avec`--revision-id`. Si quelqu'un a modifié la politique après que vous l'ayez lue, la demande échoue avec un `ConflictException` au lieu de remplacer sa modification.

Pour autoriser l'appel de tous les points de terminaison d'une fonction, utilisez un caractère générique dans l'ARN de la ressource :

```
"Resource": "arn:aws:lambda:us-east-1:111122223333:web-function/my-function/endpoint/*"
```

Remplacez la région, l'ID de compte et le nom de la fonction par vos propres valeurs. Restez `endpoint/*` à la fin.

Octroi d'une autorisation d'appel à un directeur

L'appelant doit invoquer un point `lambda:InvokeWebFunctionEndpoint` de terminaison. Pour un appelant ayant le même compte que la fonction Web, l'octroi de cette action dans la politique basée sur l'identité de l'appelant est suffisant. Aucune politique basée sur les ressources n'est requise. Pour un appelant utilisant un autre compte, cette politique basée sur l'identité est requise en plus d'une politique basée sur les ressources concernant la fonction qui l'autorise.

Associez la politique suivante au rôle ou à l'utilisateur IAM qui appellera le point de terminaison :

Example Identity-based politique pour invoquer un point de terminaison

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "lambda:InvokeWebFunctionEndpoint",
```

```
            "Resource": "arn:aws:lambda:us-east-1:111122223333:web-function/my-
function/endpoint/prod"
        }
    ]
}
```

Signature des requêtes

Lambda ne fournit pas de SDK dédié pour appeler des points de terminaison. Vous envoyez des requêtes HTTP standard et vous les signez vous-même avec SigV4 ou Sigv4a, en utilisant le nom du service. `lambda` Notez ce qui suit :

- Chaque demande signée doit inclure l'`X-Amz-Content-SHA256`en-tête, y compris les demandes sans corps. Lambda ne lit pas le corps de la demande lorsqu'il valide la signature. Il utilise donc cette valeur d'en-tête comme hachage de la charge utile. Les demandes qui ne le sont pas sont rejetées avec`403 Forbidden`.
- Si vous ne signez pas le corps (par exemple, lors du streaming), utilisez la valeur littérale `UNSIGNED-PAYLOAD` pour`X-Amz-Content-SHA256`. Lambda ne prend pas en charge la signature corporelle fragmentée.
- Lambda ne vérifie pas le corps de la requête par rapport à la `X-Amz-Content-SHA256` valeur. La signature couvre la valeur de l'en-tête, et non le contenu du corps. Si vous avez besoin d'une protection de l'intégrité corporelle allant au-delà du protocole TLS, implémentez-la dans votre application.
- Les points de terminaison régionaux (`HomeRegion`,`PerRegion`) utilisent SigV4 avec la région du point de terminaison. `MultiRegion`les points de terminaison utilisent la version 4a de AWS signature (SigV4a), qui signe pour un ensemble de régions au lieu d'une région. Utilisez l'ensemble de régions`*`.
- Si une `IamAuth` demande est renvoyée`403 Forbidden`, vérifiez qu'elle est signée avec SigV4 (ou SigV4a), qu'elle inclut l'`X-Amz-Content-SHA256`en-tête, qu'elle utilise des informations d'identification non expirées, et que vos politiques l'autorisent sur l'ARN `lambda:InvokeWebFunctionEndpoint` du point de terminaison.

Pour plus d'informations sur les demandes de signature, consultez la section Signature des demandes AWS d'API.

Une fois que Lambda a validé la signature SigV4 ou SigV4a, il supprime l'`Authorization`en-tête avant de transmettre la demande à votre fonction. Si vous souhaitez que votre fonction reçoive

l'`Authorization`en-tête d'un `IamAuth` point de terminaison, envoyez des demandes CloudFront, qui les signeront en votre nom (voirthe section called “CloudFront intégration”).

CloudFront intégration

Vous pouvez utiliser le contrôle CloudFront d'accès aux origines (OAC) d'Amazon pour placer une CloudFront distribution devant un point de `IamAuth` terminaison. Avec OAC, CloudFront signe chaque demande d'origine au nom du téléspectateur, afin que les appelants ne signent pas eux-mêmes les demandes. CloudFront n'utilise pas l'`Authorization`en-tête pour signer la demande d'origine, il peut donc transmettre votre `Authorization` en-tête à la fonction.

Lambda supprime toute `Authorization` valeur qui est elle-même une AWS signature (une valeur commençant `AWS4-` par). Cela vous permet de conserver l'authentification de votre application (par exemple, JWT ou cookies) tout en CloudFront signant chaque demande d'origine. Pour ce faire, configurez la distribution pour transférer l'`Authorization`en-tête. Pour plus d'informations, consultez Restreindre l'accès à une AWS origine.

Le domaine du point de terminaison reste accessible sur Internet, et Lambda accepte également les demandes signées directes provenant de tout principal autorisé par vos politiques.

Cela nécessite que le type d'authentification du point de terminaison soit`IamAuth`. Créez le contrôle d'accès à l'origine avec le type d'origine `lambda` et le comportement de signature`always-amz-auth`. CloudFront rejette les autres comportements de signature pour les origines des fonctions Web.

> **Note**
>
> Lambda n'authentifie pas les demandes adressées à un `ApplicationManaged` point de terminaison et n'évalue pas la politique basée sur les ressources de la fonction Web pour celles-ci. Un tel point de terminaison reste accessible au public sur son propre domaine, même en arrière CloudFront.

CloudFront Pour autoriser l'appel du point de terminaison, associez une politique basée sur les ressources à la fonction Web qui accorde l'action au principal du CloudFront service (`cloudfront.amazonaws.com`). `lambda:InvokeWebFunctionEndpoint` Utilisez une `aws:SourceArn` condition pour autoriser uniquement votre distribution spécifique :

Example Resource-based politique de l' CloudFront OAC

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCloudFrontOACAccess",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudfront.amazonaws.com"
            },
            "Action": "lambda:InvokeWebFunctionEndpoint",
            "Resource": "arn:aws:lambda:us-east-1:111122223333:web-function/my-
function/endpoint/prod",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn": "arn:aws:cloudfront::111122223333:distribution/
<distribution-id>"
                }
            }
        }
    ]
}
```

Utilisation du type **`ApplicationManaged`**d'authentification

Lorsque le type d'authentification d'un point de terminaison est défini`ApplicationManaged`, toute personne possédant le domaine du point de terminaison peut invoquer votre fonction. Lambda n'effectue aucune authentification ou autorisation.

Choisissez le `ApplicationManaged` moment où vous souhaitez que votre point de terminaison soit accessible au public, par exemple pour répondre aux demandes directement depuis un navigateur Web. Vous pouvez également le choisir lorsque vous gérez l'authentification dans votre propre code, tel que OAuth 2.0, OpenID Connect ou un schéma de jetons personnalisé.

Avec ce type d'authentification :

- Lambda permet à tous les appelants d'invoquer le point de terminaison. Il n'évalue pas de politique basée sur les ressources pour ces demandes.
- Lambda transmet l'`Authorization`en-tête de l'appelant à votre fonction, afin que votre code puisse le valider. Si l'en-tête contient une AWS signature Signature Version 4 (SigV4), Lambda la supprime, ainsi que `X-Amz-Security-Token` tout en-tête, afin AWS que les informations d'identification ne soient pas transmises à votre code de fonction.
- Votre fonction est responsable de toutes les authentifications et autorisations.

> **Note**
>
> Pour les `ApplicationManaged` points de terminaison, Lambda n'évalue pas la politique basée sur les ressources de la fonction Web pour les demandes d'appel. Vous ne pouvez pas utiliser une politique basée sur les ressources pour restreindre les personnes qui invoquent un point de terminaison. `ApplicationManaged` Pour limiter l'invocation, utilisez `IamAuth` plutôt. La politique basée sur les ressources s'applique toujours aux actions de gestion. Par exemple, il peut accorder à un autre compte l'autorisation de mettre à jour le point de terminaison. Pour plus d'informations, consultez the section called “Resource-based politiques”.

Gouvernance et contrôle d'accès

Vous pouvez contrôler qui peut configurer les points de terminaison.

Lambda prend en charge les actions IAM suivantes pour gérer les points de terminaison :

- `lambda:CreateWebFunction`— Créez une fonction Web et configurez son point de terminaison initial, y compris son`AuthType`.
- `lambda:CreateWebFunctionEndpoint`— Créez un point de terminaison et définissez-le`AuthType`.
- `lambda:UpdateWebFunctionEndpoint`— Mettez à jour un point de terminaison, y compris son`AuthType`.
- `lambda:GetWebFunctionEndpoint`— Affichez la configuration d'un point de terminaison.
- `lambda:ListWebFunctionEndpoints`— Liste les points de terminaison d'une fonction Web.
- `lambda:DeleteWebFunctionEndpoint`— Supprime un point de terminaison.

Pour autoriser ou refuser une action en fonction d'un type d'authentification, utilisez une clé de condition. `lambda:Request/WebFunctionAuthTypes`'applique à `CreateWebFunctionCreateWebFunctionEndpoint`, et`UpdateWebFunctionEndpoint`. `lambda:Resource/WebFunctionAuthTypes`'applique à `InvokeWebFunctionEndpoint` (sur les `IamAuth` points de terminaison)`UpdateWebFunctionEndpoint`,`GetWebFunctionEndpoint`, et`DeleteWebFunctionEndpoint`. Pour plus de détails, consultez the section called “Clés de condition”.

Restreindre les points de terminaison publics dans une organisation

Si vous administrez une AWS organisation et souhaitez empêcher les développeurs de créer des points de terminaison publics, utilisez une politique de contrôle des services (SCP) qui interdit de créer ou de mettre à jour des points de terminaison avec le `ApplicationManaged` type d'authentification. Utilisez la clé de `lambda:Request/WebFunctionAuthType` condition, qui reflète le type d'authentification dans la demande :

Example Le SCP refuse les points de terminaison publics

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "lambda:CreateWebFunction",
                "lambda:CreateWebFunctionEndpoint",
                "lambda:UpdateWebFunctionEndpoint"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "lambda:Request/WebFunctionAuthType": "ApplicationManaged"
                }
            }
        }
    ]
}
```

La politique inclut le `lambda:CreateWebFunction` fait que cette opération crée le point de terminaison initial à partir de celui de la demande`endpointConfig`. Lorsque cette politique est en place, `aws lambda-web deploy` échoue avec une erreur de refus d'accès, sauf si le développeur l'ajoute`--auth-type IamAuth`. Par défaut, la commande crée un `ApplicationManaged` point de terminaison.

Clés de condition

Pour un contrôle d'accès précis, Lambda prend en charge les clés de contexte de condition suivantes :

- `lambda:Request/WebFunctionAuthType`— Le type d'authentification spécifié dans une demande. Disponible pendant `CreateWebFunction`CreateWebFunctionEndpoint, et`UpdateWebFunctionEndpoint`. Utilisez-le pour contrôler les types d'authentification qui peuvent être configurés.
- `lambda:Resource/WebFunctionAuthType`— Le type d'authentification actuellement configuré sur un terminal, avec les valeurs `IamAuth` et`ApplicationManaged`. Disponible pendant `InvokeWebFunctionEndpoint`UpdateWebFunctionEndpoint,`DeleteWebFunctionEndpoint`, et`GetWebFunctionEndpoint`. En effet`InvokeWebFunctionEndpoint`, Lambda évalue la clé uniquement sur les points de terminaison, car les demandes adressées aux `IamAuth` points de `ApplicationManaged` terminaison ne sont pas autorisées par IAM.
- `aws:ResourceTag/${TagKey}`— Filtre l'accès par les balises de la fonction Web. Les points de terminaison et les révisions héritent des balises de la fonction parent. Vous pouvez donc utiliser ABAC pour contrôler l'accès aux appels.

Example Autoriser l'invocation uniquement sur les points de terminaison d'une fonction balisée

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "lambda:InvokeWebFunctionEndpoint",
            "Resource": "arn:aws:lambda:us-east-1:111122223333:web-function/*/endpoint/
prod",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Environment": "Production"
                }
            }
        }
    ]
}
```

Chiffrement au repos pour les fonctions Web

AWS Lambda chiffre les données de vos fonctions Web Lambda au repos côté serveur. Cette page explique les options de chiffrement à votre disposition et explique comment configurer une clé gérée par le client.

Options de chiffrement au repos

Le chiffrement au repos est toujours activé. Lambda chiffre votre artefact de code de fonction Web et vos variables d'environnement côté serveur, et vous ne pouvez pas désactiver ce chiffrement. Par défaut, Lambda utilise un. Clé détenue par AWS Vous pouvez plutôt configurer une clé gérée par le client.

Deux options s'offrent à vous pour choisir la AWS KMS clé qui protège vos données :

Clé détenue par AWS (default)

Par défaut, Lambda chiffre vos données à l'aide d'un. Clé détenue par AWS AWS possède et gère cette clé. Vous ne pouvez pas consulter, gérer ou auditer son utilisation. Si ce comportement par défaut répond à vos besoins, aucune configuration supplémentaire n'est requise.

Clé gérée par le client

Vous pouvez éventuellement configurer votre propre clé gérée par AWS KMS le client. Utilisez une clé gérée par le client lorsque vous devez contrôler la rotation des clés, vérifier l'utilisation des clés CloudTrail, gérer l'accès aux clés par le biais d'une politique clé ou répondre aux exigences de conformité de l'organisation. Avec une clé gérée par le client, seuls les principaux que vous autorisez peuvent accéder au code crypté et aux variables d'environnement. Les clés gérées par le client entraînent des AWS KMS frais. Pour en savoir plus, consultez Pricing AWS Key Management Service (Tarification).

Chiffrer les données au repos à l'aide d'une clé gérée par le client

Les sections suivantes expliquent comment les fonctions Web utilisent une clé gérée par le client, comment configurer la clé et ses autorisations, et comment limiter l'accès à celle-ci.

Comment les fonctions Web utilisent une clé gérée par le client

Lorsque vous spécifiez une clé gérée par le client, Lambda utilise le chiffrement d'enveloppe. Cela signifie que Lambda chiffre les données de la révision à l'aide d'une clé de données, et votre clé KMS chiffre cette clé de données. Lambda obtient la clé de données AWS KMS et la déchiffre avec votre clé KMS lorsqu'il a besoin de lire les données. Seuls les principaux ayant accès à la clé KMS peuvent accéder au code et aux variables d'environnement de la révision.

Lambda chiffre les ressources de fonctions Web suivantes à l'aide de votre clé gérée par le client :

Ressource	Qu'est-ce qui est crypté
Révision	L'artefact de code créé à partir de votre package de déploiement Amazon S3 et les variables d'environnement de la révision.

Lambda n'utilise pas de privilèges pour AWS KMS les fonctions Web. L'accès est autorisé par le biais de la politique des clés et des autorisations IAM du principal appelant.

Lambda appelle AWS KMS lors de la création et du lancement de ressources de révision et peut mettre en cache du matériel déchiffré dans des environnements d'exécution actifs. La révocation de l'accès par clé n'est pas un mécanisme immédiat de limitation du trafic, car les environnements existants peuvent continuer à utiliser du matériel mis en cache pendant une période indéterminée.

Après un changement de politique clé, testez le comportement attendu et surveillez la révision et l'état du terminal. Pour le confinement d'urgence, arrêtez d'acheminer le trafic vers les révisions concernées ou désactivez le point de terminaison au lieu de vous fier uniquement à la révocation des clés.

Lambda définit le contexte de chiffrement suivant pour toutes les AWS KMS opérations relatives aux fonctions Web :

- `aws:lambda:WebFunctionRevisionArn`— Le nom de ressource Amazon (ARN) de la révision de la fonction Web.

Vous pouvez utiliser ce contexte de chiffrement dans les politiques clés pour définir l'accès à des fonctions Web ou à des révisions spécifiques. Pour plus d’informations, consultez the section called “Délimitation de l'accès à votre clé KMS”.

Configuration d'une clé gérée par le client

La AWS KMS clé doit être une clé de chiffrement symétrique (spécification de la clé`SYMMETRIC_DEFAULT`, utilisation `ENCRYPT_DECRYPT` de la clé). Vous ne pouvez pas utiliser de touches asymétriques.

Les fonctions Web prennent en charge les touches multirégionales. Le type de clé dont vous avez besoin dépend de la configuration de votre terminal :

- HomeRegion point de terminaison : vous pouvez utiliser une clé à région unique ou une clé multirégionale.
- MultiRegion ou PerRegion point de terminaison : vous devez utiliser une clé multirégionale avec des répliques dans chaque Région AWS point desservi par le point de terminaison. Si une région ne possède pas de réplique de la clé, la réplication vers cette région échoue.

Pour plus d'informations sur la création de clés multirégionales, voir Création de clés primaires multirégionales dans le guide du AWS Key Management Service développeur.

Comme il AWS KMS ne copie ni ne synchronise les politiques clés entre les clés multirégionales associées, vous devez configurer chaque stratégie clé séparément. Configurez la politique des clés sur la clé primaire et sur chaque clé de réplique. Au minimum, la politique de chaque clé de réplique doit autoriser le principal du service Lambda à appeler. `kms:Decrypt` Cette autorisation permet à Lambda de déchiffrer la clé de données dans cette région. Pour plus d'informations, consultez la section Autorisation de l'utilisation de clés multirégionales dans le Guide du AWS Key Management Service développeur.

> **Note**
>
> Lorsque vous créez des répliques de clés multirégionales, leur disponibilité dans toutes les régions peut prendre de quelques secondes à quelques minutes. Vérifiez que la clé de réplique est disponible dans chaque région cible avant de créer la révision ou le point de terminaison.

Configuration des autorisations pour utiliser une clé gérée par le client

Pour créer une révision à l'aide d'une clé gérée par le client, vous devez disposer des autorisations suivantes sur la AWS KMS clé :

- `kms:DescribeKey`— Obligatoire lorsque vous créez une fonction Web ou une révision à l'aide de la clé.
- `kms:GenerateDataKey`— Lambda appelle cette opération pour générer la clé de données qui chiffre l'artefact de code et les variables d'environnement de la révision.
- `kms:Decrypt`— Lambda appelle cette opération pour valider que la clé est utilisable lorsque vous créez la révision. Les directeurs qui lisent une révision doivent `GetWebFunctionRevision` également avoir `kms:Decrypt` la clé pour voir ses variables d'environnement.

La demande de création échoue si la clé est manquante, désactivée, s'il ne s'agit pas d'une clé de chiffrement symétrique ou si elle n'est pas accessible avec les autorisations requises.

> **Note**
>
> Vous n'avez pas besoin d'`kms:Encrypt`autorisation. Lambda utilise le chiffrement d'enveloppe avec`GenerateDataKey`, qui renvoie à la fois un texte brut et une copie cryptée de la clé de données sans nécessiter un appel de chiffrement distinct.

La politique AWS KMS des clés doit également autoriser le principal du service Lambda (`lambda.amazonaws.com`) à appeler. `kms:Decrypt` Lambda utilise cette autorisation pour déchiffrer la clé de données lorsqu'il lance des environnements d'exécution pour la révision. Le directeur du service n'en a pas besoin`kms:DescribeKey`. Le principal qui crée la fonction Web ou la révision a besoin de cette autorisation.

Exemple de politique de clé

La politique clé suivante contient les trois instructions requises par les fonctions Web, chacune étant limitée aux conditions décrites dansthe section called “Délimitation de l'accès à votre clé KMS”. La première instruction accorde au principal du service Lambda les autorisations dont il a besoin lorsqu'il lance des environnements d'exécution. Les deuxième et troisième accordent au directeur qui crée les révisions les autorisations dont il a besoin au moment de la création.

`kms:DescribeKey`figure dans une instruction séparée car il s'agit d'une opération de métadonnées qui ne comporte aucun contexte de chiffrement. Une condition de contexte de chiffrement ne correspondrait jamais à une `DescribeKey` demande, de sorte que cette condition ne s'applique qu'à l'instruction qui accorde `kms:GenerateDataKey` et`kms:Decrypt`.

Cet exemple montre uniquement les instructions dont Lambda a besoin pour les fonctions Web. Ajoutez ces instructions à votre politique clé existante plutôt que de la remplacer, et conservez les instructions qui accordent à vos administrateurs l'accès à la gestion de la clé.

Example Politique clé pour le chiffrement des fonctions Web

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow Lambda to decrypt the data key for Web Function revisions",
```

```
            "Effect": "Allow",
            "Principal": { "Service": "lambda.amazonaws.com" },
            "Action": "kms:Decrypt",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "kms:EncryptionContext:aws:lambda:WebFunctionRevisionArn":
 "arn:aws:lambda:us-east-1:111122223333:web-function/my-function/revision/*",
                    "aws:SourceArn": "arn:aws:lambda:us-east-1:111122223333:web-
function/my-function/revision/*"
                }
            }
        },
        {
            "Sid": "Allow the revision creator to generate and validate data keys",
            "Effect": "Allow",
            "Principal": { "AWS":
 "arn:aws:iam::111122223333:role/MyWebFunctionDeployRole" },
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "kms:EncryptionContext:aws:lambda:WebFunctionRevisionArn":
 "arn:aws:lambda:us-east-1:111122223333:web-function/my-function/revision/*"
                },
                "StringEquals": {
                    "kms:ViaService": "lambda.us-east-1.amazonaws.com"
                }
            }
        },
        {
            "Sid": "Allow the revision creator to describe the key",
            "Effect": "Allow",
            "Principal": { "AWS":
 "arn:aws:iam::111122223333:role/MyWebFunctionDeployRole" },
            "Action": "kms:DescribeKey",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "lambda.us-east-1.amazonaws.com"
                }
```

```
            }
        }
    ]
}
```

Pour plus d'informations sur les politiques AWS KMS clés, consultez la section Politiques clés du Guide du AWS Key Management Service développeur. AWS KMS

Création d'une révision de fonction Web à l'aide d'une clé gérée par le client

Pour chiffrer une révision à l'aide d'une clé gérée par le client, spécifiez l'ARN de la clé dans le `kmsKeyArn` paramètre de configuration de révision. Vous pouvez définir ce paramètre lorsque vous appelez CreateWebFunctionou CreateWebFunctionRevision. Si vous omettez`kmsKeyArn`, Lambda chiffre la révision à l'aide du. Clé détenue par AWS

Pour créer une fonction Web avec une clé gérée par le client (AWS CLI)

- Exécutez la commande suivante pour créer une fonction Web avec une clé gérée par le client.

```
aws lambda-web create-web-function \
    --function-name my-web-app \
    --revision-config '{
      "kmsKeyArn": "arn:aws:kms:us-east-1:111122223333:key/key-id",
      "buildConfig": {
        "codeConfig": {
          "s3Object": { "bucket": "amzn-s3-demo-bucket", "key": "my-app.zip" }
        },
        "runtimeConfig": { "runtime": "nodejs24.x" }
      },
      "serviceConfig": {
        "executionRoleArn": "arn:aws:iam::111122223333:role/my-web-function-role"
      }
    }' \
    --endpoint-config '{
      "endpointName": "my-endpoint",
      "endpointType": "HomeRegion",
      "authType": "ApplicationManaged"
    }'
```

Modification de la configuration de chiffrement d'une fonction Web existante

Le `kmsKeyArn` paramètre est fixe pendant toute la durée de vie d'une révision. Les révisions étant immuables, vous ne pouvez pas modifier la clé qui protège une révision existante. Pour modifier la configuration du chiffrement, créez une nouvelle révision qui spécifie la nouvelle clé, puis acheminez le trafic vers cette révision.

Les fonctions Web prennent en charge les transitions clés suivantes :

- Clé détenue par AWS à la clé gérée par le client — Créez une nouvelle révision qui spécifie`kmsKeyArn`.
- Une clé gérée par le client vers une autre clé gérée par le client : créez une nouvelle révision qui spécifie le nouvel ARN de la clé.
- Clé gérée par le client pour Clé détenue par AWS — Créer une nouvelle révision sans`kmsKeyArn`. Lambda protège ensuite cette révision avec le Clé détenue par AWS, qui est la valeur par défaut.

Lambda ne rechiffre pas les révisions existantes lorsque vous créez une nouvelle révision avec une clé différente. Chaque révision reste cryptée avec la clé que vous avez spécifiée lors de sa création. Cela signifie que tant qu'une version antérieure peut encore recevoir du trafic, sa clé d'origine doit rester activée et accessible au principal du service Lambda. Avant de désactiver ou de supprimer une clé, vérifiez qu'aucune révision chiffrée avec cette clé n'est toujours référencée par les poids de révision d'un point de terminaison.

Pour créer une nouvelle révision avec une autre clé gérée par le client (AWS CLI)

1. Exécutez la commande suivante pour créer une révision utilisant une clé différente.

```
aws lambda-web create-web-function-revision \
    --function-name my-web-app \
    --kms-key-arn arn:aws:kms:us-east-1:111122223333:key/new-key-id \
    --build-config '{
      "codeConfig": { "s3Object": { "bucket": "my-bucket", "key": "my-app-
v2.zip" } },
      "runtimeConfig": { "runtime": "nodejs24.x" }
    }' \
    --service-config '{
      "executionRoleArn": "arn:aws:iam::111122223333:role/my-web-function-role"
    }'
```

2. Mettez à jour les poids de révision du point de terminaison pour acheminer le trafic vers la nouvelle révision. Pour plus d'informations, consultez the section called "Modèles de déploiement".

Délimitation de l'accès à votre clé KMS

La politique clé de the section called "Exemple de politique de clé" restreint l'accès avec les clés de condition suivantes. Chacune limite la manière dont la clé peut être utilisée, de sorte que l'accès à la clé ne soit pas plus large que ce dont la fonction Web a besoin.

Contexte de chiffrement

Lambda définit le contexte `aws:lambda:WebFunctionRevisionArn` de chiffrement pour chaque AWS KMS demande de révision. Utilisez une `StringLike` condition activée `kms:EncryptionContext:aws:lambda:WebFunctionRevisionArn` pour limiter la clé aux révisions d'une fonction Web spécifique. Appliquez cette condition à la fois à la déclaration du créateur et à la déclaration principale du service Lambda.

N'appliquez pas cette condition à une déclaration qui accordekms:DescribeKey. Cette opération ne comporte aucun contexte de chiffrement, de sorte que la condition la refuserait.

L'exemple suivant montre l'instruction creator avec la condition de contexte de chiffrement.

```
{
    "Sid": "Allow the revision creator to generate and validate data keys",
    "Effect": "Allow",
    "Principal": { "AWS": "arn:aws:iam::111122223333:role/MyWebFunctionDeployRole" },
    "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt"
    ],
    "Resource": "*",
    "Condition": {
        "StringLike": {
            "kms:EncryptionContext:aws:lambda:WebFunctionRevisionArn":
 "arn:aws:lambda:us-east-1:111122223333:web-function/my-function/revision/*"
        }
    }
}
```

km : ViaService état

La `kms:ViaService` condition restreint la clé afin que seules les demandes que Lambda fait en votre nom puissent l'utiliser. La valeur est Region-specific :`lambda.us-east-1.amazonaws.com`.

Avec cette condition, AWS KMS refuse les appels directs effectués avec les mêmes informations d'identification (par exemple, s'exécuter `aws kms generate-data-key` vous-même), mais la création d'une fonction Web aboutit car Lambda passe AWS KMS les appels pour vous.

AWS KMS ne partage pas les politiques clés entre les clés multirégionales associées. Chaque clé de réplique possède sa propre politique. Lorsque vous utilisez la `kms:ViaService` condition avec une clé multirégionale, utilisez le nom du service régional qui correspond à la région de chaque clé (par exemple, `lambda.us-east-1.amazonaws.com` dans la politique de clé us-east-1 et `lambda.us-west-2.amazonaws.com` dans la politique de clé de réplique us-west-2). Vous pouvez également répertorier plusieurs valeurs régionales dans une seule condition, car elle `StringEquals` accepte un tableau de valeurs.

L'exemple suivant montre l'instruction creator avec à la fois la `kms:ViaService` condition et la condition de contexte de chiffrement.

```
{
    "Sid": "Allow the revision creator to generate and validate data keys",
    "Effect": "Allow",
    "Principal": { "AWS": "arn:aws:iam::111122223333:role/MyWebFunctionDeployRole" },
    "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt"
    ],
    "Resource": "*",
    "Condition": {
        "StringLike": {
            "kms:EncryptionContext:aws:lambda:WebFunctionRevisionArn":
 "arn:aws:lambda:us-east-1:111122223333:web-function/my-function/revision/*"
        },
        "StringEquals": {
            "kms:ViaService": "lambda.us-east-1.amazonaws.com"
        }
    }
}
```

Protection adjointe confuse

Le problème des adjoints confus se produit lorsqu'une entité non autorisée à effectuer une action contraint une entité plus privilégiée à l'exécuter. Étant donné que le responsable du service Lambda peut utiliser votre clé gérée par le client, limitez cet accès aux révisions des fonctions Web dont vous êtes propriétaire. Pour de plus amples informations, veuillez consulter Le problème du député confus dans le Guide de l'utilisateur IAM.

Lorsque Lambda appelle AWS KMS avec ses propres informations d'identification de service pour lancer un environnement d'exécution, il envoie l'ARN de révision en tant qu'ARN source et votre Compte AWS identifiant en tant que compte source. Utilisez la clé aws : SourceArn condition sur l'instruction principale du service Lambda pour restreindre la clé aux révisions d'une fonction Web spécifique.

```
{
    "Sid": "Allow Lambda to decrypt the data key for Web Function revisions",
    "Effect": "Allow",
    "Principal": { "Service": "lambda.amazonaws.com" },
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
        "StringLike": {
            "aws:SourceArn": "arn:aws:lambda:us-east-1:111122223333:web-function/my-
function/revision/*"
        }
    }
}
```

Pour restreindre la clé à votre compte plutôt qu'à une fonction Web spécifique, utilisez la clé de SourceAccount condition aws : avec votre Compte AWS identifiant.

Appliquez cette condition à la déclaration principale du service Lambda. La `kms:ViaService` condition décrite dans the section called “km : ViaService état” limite le service autorisé à utiliser la clé, mais elle ne crée pas de confusion quant à la protection des adjoints.

Comportement d'erreur

Lambda valide la AWS KMS clé lorsque vous créez une révision. Les erreurs suivantes peuvent se produire au moment de la création :

- Erreur de validation — L'ARN de la clé n'est pas valide, la clé n'existe pas, la clé est désactivée ou la clé n'est pas une clé de chiffrement symétrique.
- Erreur d'accès refusé — Le principal appelant ou le principal du service Lambda ne dispose pas des AWS KMS autorisations requises sur la clé.

⚠ Ne pas désactiver ou révoquer l'accès à la clé d'une révision active

Si vous désactivez la AWS KMS clé ou révoquez l'accès du principal du service Lambda après une révision`Active`, Lambda ne peut plus déchiffrer la clé de données. Cela empêche Lambda de lancer de nouveaux environnements d'exécution pour cette révision, ce qui interrompt les invocations. Ne supprimez pas non plus les clés de réplique dans les régions où la révision est toujours déployée. Cela a le même effet (Lambda ne peut pas lancer de nouveaux environnements d'exécution dans cette région). Pour rétablir le service, créez une nouvelle révision avec une clé accessible, ou réactivez la clé d'origine et restaurez la politique de clé.

Chiffrement avec MultiRegion et points de PerRegion terminaison

Pour les fonctions Web avec MultiRegion ou PerRegion points de terminaison, Lambda vérifie la disponibilité des clés dans chaque région lors de la réplication. Si la réplique clé multirégionale est manquante ou inaccessible dans une région cible, la réplication échoue uniquement pour cette région. Les autres régions continuent de fonctionner normalement.

Vous pouvez consulter l'état de chaque région et le mettre à jour en appelant`GetWebFunctionEndpoint`. L'entrée de chaque région `regionalEndpoints` contient `state` et `stateReason` (l'état de déploiement de la région) `updateStatus` et `updateStatusReason` (le résultat de la dernière mise à jour). Le comportement varie selon que le point de terminaison est créé ou mis à jour :

- Lors de la création du point de terminaison : l'entrée de la région `regionalEndpoints` indique un `state` de `Failed` avec un `stateReason` qui décrit le problème clé. Le point de terminaison global `Failed` s'affiche `state` également et vous `stateReason` dirige vers les entrées régionales.
- Lors d'une mise à jour d'un terminal, la région `updateStatusReason` s'`updateStatus`affiche `Failed` avec un message décrivant le principal problème. Le point de terminaison global `Failed`

s'affiche `updateStatus` également et vous `updateStatusReason` dirige vers les entrées régionales.

Pour résoudre une région défaillante, créez une réplique clé dans cette région ou restaurez l'accès à la réplique existante, puis mettez à jour le point de terminaison pour réessayer la réplication.

Surveillance de l'interaction des fonctions Web avec AWS KMS

Vous pouvez l'utiliser CloudTrail pour suivre les AWS KMS demandes que Lambda fait en votre nom lorsque vous utilisez une clé gérée par le client avec une fonction Web. Pour plus d'informations sur la recherche d' AWS KMS événements dans vos CloudTrail journaux, consultez la section Rechercher CloudTrail des appels AWS KMS d'API dans les journaux du guide du AWS Key Management Service développeur.

Le tableau suivant répertorie les AWS KMS événements générés par les fonctions Web et les valeurs que vous pouvez auditer pour chaque événement.

eventName	Quand cela se produit	Valeurs à auditer
`DescribeKey`	Lorsque vous créez une fonction Web ou une révision à l'aide d'une clé gérée par le client.	`userIdentity` est le principal IAM qui a créé la révision. Cet événement n'a aucun contexte de chiffrement, car il `DescribeKey` s'agit d'une opération de métadonnées.
`GenerateDataKey`	Lorsque vous créez une fonction Web ou une révision. Lambda génère la clé de données qui chiffre l'artefact de code et les variables d'environnement de la révision.	`userIdentity` est le principal IAM qui a créé la révision. `encryptionContext` contient`aws:lambda:WebFunctionRevisionArn` .
`Decrypt`	Lorsque vous créez une fonction Web ou une révision, Lambda valide l'accès par clé. Lambda appelle également cette opération lorsqu'il déploie la révision dans une région de réplique, lorsqu'il lance un nouvel environnement d'exécution et	Pour les appels au moment de la création, `userIdentity` c'est le principal IAM qui a créé la révision. Lambda effectue également un `Decrypt` appel à sec `lambda.amazonaws.com` pour confirmer que le directeur du service peut

eventName	Quand cela se produit	Valeurs à auditer
	lorsqu'un appelant lit les variables d'environnement de la révision avec. `GetWebFunctionRevision`	utiliser la clé. Pour les appels d'exécution, `userIdentity` c'est le principal du service Lambda ()`lambda.amazonaws.com` . En effet`GetWebFunctionRevision` , Lambda appelle `Decrypt` avec les informations d'identification de l'appelant. `encryptionContext` contient`aws:lambda:WebFunctionRevisionArn` .

Les `Decrypt` événements `GenerateDataKey` et incluent le contexte de chiffrement `aws:lambda:WebFunctionRevisionArn` avec l'ARN de révision. Utilisez cette valeur pour identifier les AWS KMS demandes de révision d'une fonction Web spécifique.

Surveillance des fonctions Web Lambda

AWS Lambda Les fonctions Web publient des statistiques et des journaux sur Amazon CloudWatch. Utilisez-les pour identifier les problèmes de performance, les erreurs de débogage et définir des alarmes qui vous alertent lorsque le taux d'erreur augmente lors des déploiements Canary ou des changements de trafic.

Pour une fonction Web qui traite des demandes dans plusieurs cas Région AWS, Lambda collecte des métriques et des journaux dans chaque région où les demandes sont exécutées. Il centralise les métriques des demandes et se connecte à la région d'origine de la fonction Web, afin que vous puissiez surveiller l'ensemble de l'application à partir d'un seul endroit. Les indicateurs d'utilisation et de limitation restent dans la région où ils sont émis, car les quotas qu'ils décrivent s'appliquent par région.

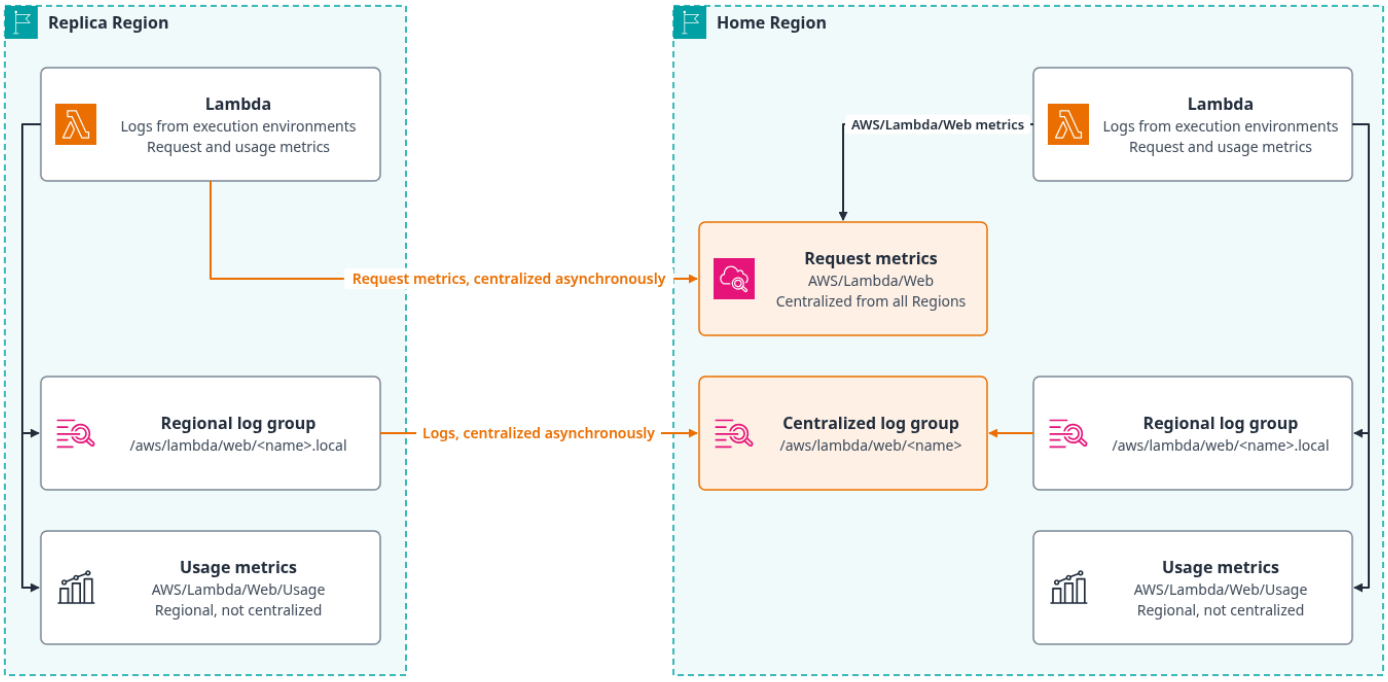
Chaque type de télémétrie répond à une question différente :

- Métriques : suivez les performances de votre fonction Web au fil du temps et alertez en cas de problème. Pour plus de détails, consultez the section called “Métriques”.
- Journaux : examinez les demandes et les erreurs individuelles. Pour plus de détails, consultez the section called “Journaux”.

- Métriques personnalisées : publiez vos propres métriques d'application en écrivant le format de métrique intégré dans vos journaux. Pour plus de détails, consultez the section called “Métriques personnalisées”.
- CloudTrail— Enregistrez les appels d'API pour vos fonctions Web, y compris les invocations, qui sont enregistrées sous forme d' CloudTrail événements de données. Pour plus de détails, consultez the section called “CloudTrail journaux”.

Pour résoudre les problèmes dans la région où une demande a été exécutée, utilisez le groupe de journaux régional`/aws/lambda/web/`*`function-name`*`.local`, dans lequel les environnements d'exécution rédigent des journaux. Lambda centralise les journaux de manière asynchrone dans le groupe de journaux de la région d'`/aws/lambda/web/`*`function-name`*origine. Pour plus d'informations sur les régions d'origine et la réplication, consultezthe section called “Multi-Region déploiement”.

Le schéma suivant montre comment Lambda écrit et centralise la télémétrie entre les régions. Les métriques de demande dans l'espace de `AWS/Lambda/Web` noms et les journaux sont centralisées dans la région d'origine. Les métriques d'utilisation de l'espace de `AWS/Lambda/Web/Usage` noms restent dans chaque région.



Rubriques

- Facturation par télémétrie

- Considérations relatives à la télémétrie
- Utilisation de CloudWatch métriques avec les fonctions Web Lambda
- Journaux des fonctions Web dans Amazon CloudWatch Logs
- Publication de métriques personnalisées avec le format de métrique intégré
- Journalisation des appels d'API de fonction Web à l'aide de AWS CloudTrail

Facturation par télémétrie

La télémétrie pour les fonctions Web est facturée comme suit :

Télémétrie	Facturation
Métriques publiées par Lambda	Gratuit. Lambda publie les métriques dans les `AWS/Lambda/Web/Usage` espaces de noms `AWS/Lambda/Web` et sans frais pour vous.
Journaux	Vous payez CloudWatch les frais Amazon Logs standard pour écrire et stocker des journaux dans le groupe de `.local` journaux de chaque région. Vous payez également pour stocker les copies dans le groupe de journaux centralisé de la région d'origine. Lambda copie gratuitement chaque événement du journal dans la région d'origine. La première centralisation du journal des événements est gratuite.
Métriques personnalisées	Les métriques personnalisées que vous publiez à l'aide du format de métrique intégré entraînent des frais d'ingestion Amazon CloudWatch Logs et des frais de métriques CloudWatch personnalisés. La première centralisation du journal des événements est gratuite. Pour plus d'informations, consultez the section called “Métriques personnalisées”.

Pour les prix actuels, consultez les CloudWatchtarifs Amazon.

Considérations relatives à la télémétrie

Passez en revue les comportements suivants avant de créer des tableaux de bord, des alarmes ou des automatismes sur la télémétrie des fonctions Web.

AWS X-Ray suivi

Si une demande inclut un `X-Amzn-Trace-Id` en-tête, Lambda le transmet sans modification à votre application. Lambda n'ajoute pas d'en-tête de trace aux demandes qui n'en incluent pas, et les fonctions Web ne créent pas de segments de service Lambda. Étant donné que les appelants définissent cet en-tête, considérez sa valeur comme une entrée client. Pour enregistrer des traces, envoyez les données de trace de votre code directement à X-Ray, par exemple avec le AWS Distro for OpenTelemetry, et autorisez votre rôle d'exécution à écrire sur X-Ray.

Latence de centralisation

Les métriques et les journaux atteignent la région d'origine de manière asynchrone. En régime permanent, Lambda centralise généralement les métriques et les journaux en quelques minutes. La télémétrie peut arriver plus tard lors d'une interruption de service.

Lorsque vous créez un point de terminaison qui s'exécute dans plusieurs régions, Lambda configure la centralisation des métriques pour chaque région de réplication. CloudWatch plusieurs minutes peuvent s'écouler une fois que le point de terminaison est devenu actif dans une région pour commencer à centraliser ses indicateurs à partir de cette région. Les métriques émises avant cette date restent uniquement dans cette région et ne sont pas ajoutées ultérieurement à la région d'origine.

Tenez compte de cette latence dans l'automatisation du déploiement. Si un pipeline crée une fonction Web ou un point de terminaison, puis vérifie immédiatement les métriques ou les journaux dans la région d'origine, laissez le temps à la première télémétrie d'arriver plutôt que de considérer son absence comme un échec.

Télémétrie dans chaque région

Lambda écrit la télémétrie dans chaque région où les demandes sont exécutées, puis en centralise une partie dans la région d'origine. Ce sur quoi vous pouvez compter dans chaque région dépend du type de télémétrie :

Métriques des demandes (`AWS/Lambda/Web`)

Lambda peut également écrire ces métriques dans d'autres régions où les demandes sont exécutées. Ils peuvent être modifiés ou supprimés sans préavis. Nous vous recommandons donc de ne pas vous y fier et d'utiliser plutôt les valeurs centralisées de la région d'origine pour les alarmes, les tableaux de bord et l'automatisation. Les valeurs centralisées incluent les demandes provenant de chaque région desservie par le point de terminaison.

Métriques d'utilisation et de limitation () `AWS/Lambda/Web/Usage`

Ces indicateurs n'existent que dans la région où la demande a été traitée. Alarme sur eux dans chaque région. Pour plus de détails, consultez the section called “Indicateurs régionaux d'utilisation et de limitation”.

Journaux

Dans chaque région, le groupe de `.local` journaux contient uniquement les journaux de cette région. Ces journaux sont disponibles avant la fin de la centralisation et ne sont pas affectés par les délais de centralisation, ce qui les rend utiles pour résoudre un problème régional. Le groupe de journaux centralisé de la région d'origine contient les journaux de chaque région. Créez des requêtes partagées, des abonnements et des politiques de rétention sur le groupe de journaux centralisé. Pour plus de détails, consultez the section called “Groupes de journaux”.

Interruptions de service

Les perturbations de l'infrastructure, telles qu'une panne de zone de disponibilité, peuvent retarder la télémétrie, et certains indicateurs et événements du journal peuvent être perdus. Si la région d'origine est affectée, les statistiques et les journaux centralisés dans la région d'origine peuvent être retardés ou indisponibles. Les mesures d'utilisation et les groupes de `.local` journaux dans les autres régions ne dépendent pas de la centralisation et continuent de recevoir des données télémétriques provenant de ces régions.

La télémétrie est émise dans la mesure du possible. Dans de rares cas, la télémétrie peut être supprimée ou dupliquée. Ne considérez pas la télémétrie des fonctions Web comme un enregistrement d'audit. Pour auditer les modifications de configuration et les appels, utilisez. AWS CloudTrail Pour plus d’informations, consultez the section called “CloudTrail journaux”.

Autorisations nécessaires

La journalisation nécessite les autorisations Amazon CloudWatch Logs `logs:CreateLogGrouplogs:CreateLogStream`, et `logs:PutLogEvents` dans le rôle

d'exécution de votre fonction Web. Sans eux, Lambda ne peut pas créer de groupes de journaux ni écrire des événements de journal, et la sortie de votre application est perdue. Pour un exemple de politique, consultez the section called “Rôle d'exécution”.

Lambda publie les métriques dans les `AWS/Lambda/Web/Usage` espaces de noms `AWS/Lambda/Web` et eux-mêmes, elles n'ont donc pas besoin d'autorisation dans le rôle d'exécution, y compris. `cloudwatch:PutMetricData` Le format de métrique intégré n'appelle pas `PutMetricData` directement, mais il nécessite les mêmes autorisations Amazon CloudWatch Logs, car Lambda extrait les métriques de vos événements de journal.

Utilisation de CloudWatch métriques avec les fonctions Web Lambda

AWS Lambda publie les métriques des fonctions Web sur Amazon CloudWatch dans deux espaces de noms :

- `AWS/Lambda/Web`— Mesures de demande et de réponse pour chaque point de terminaison, et mesures d'utilisation des ressources pour les environnements d'exécution qui desservent chaque fonction Web. Lambda centralise ces mesures dans la région d'origine de la fonction Web, de sorte que les valeurs de cette région incluent le trafic provenant de chaque région desservie par le point de terminaison.
- `AWS/Lambda/Web/Usage`— Indicateurs régionaux d'utilisation et de limitation qui montrent la consommation par rapport aux quotas régionaux et aux limites des terminaux. Ces indicateurs ne sont pas centralisés. Ils restent dans la région où la demande a été envoyée.

Lambda publie les métriques de demande, d'utilisation et de limitation uniquement lorsqu'une requête produit une valeur pour celles-ci. Les métriques de l'environnement d'exécution sont différentes : Lambda les publie toutes les minutes pour chaque environnement d'exécution actif. Certaines mesures sont rares : Lambda ne publie pas de point de données égal à 0 pour une période au cours de laquelle l'événement ne s'est pas produit. Par exemple, si aucune demande ne renvoie de réponse 5xx au cours d'une période, `HTTPResponseStatusClass5XX` elle n'a aucun point de données pour cette période. Les tableaux suivants décrivent à quel moment Lambda émet chaque métrique. Lorsque vous créez des alarmes sur des métriques éparses, configurez la façon dont l'alarme traite les données manquantes. Pour plus d'informations, consultez la section Configuration de la manière dont les CloudWatch alarmes traitent les données manquantes dans le guide de CloudWatch l'utilisateur Amazon.

Rubriques

- Métriques des demandes
- Métriques de l'environnement d'exécution
- Indicateurs régionaux d'utilisation et de limitation
- Utilisation des métriques avec d'autres CloudWatch fonctionnalités
- Régler une alarme sur les réponses 5xx

Métriques des demandes

Les métriques de demande sont publiées dans l'espace de `AWS/Lambda/Web` noms avec les `EndpointName` dimensions `FunctionName` et. Ils utilisent l'`Count`unité. Utilisez les `Sum` statistiques.

Métrique	Statistique	Quand Lambda l'émet	Description
`ExecutedRequests`	`Sum`	Uniquement pour les périodes au cours desquelles au moins une demande a atteint un environnement d'exécution.	Le nombre de demandes qui ont atteint un environnement d'exécution. Les demandes que Lambda limite ou rejette avant d'atteindre un environnement d'exécution ne sont pas prises en compte.
`HTTPResponseStatusClass4XX`	`Sum`	clairsemé. Uniquement pour les périodes avec au moins une réponse 4xx.	Le nombre de réponses renvoyées aux appelants avec un code d'état compris entre 400 et 499. La réponse peut provenir de votre application ou de Lambda, y compris les requêtes limitées qui reçoivent le protocole HTTP 429. Les demandes rejetées par Lambda avant d'identifier le point de terminaison, telles que les demandes mal formées, ne sont pas prises en compte.

Métrique	Statistique	Quand Lambda l'émet	Description
`HTTPResponseStatusClass5XX`	`Sum`	clairsemé. Uniquement pour les périodes avec au moins une réponse 5xx.	Le nombre de réponses renvoyées aux appelants avec un code d'état compris entre 500 et 599. La réponse peut provenir de votre application ou de Lambda. Lors d'une interruption de service, cette métrique peut sous-estimer le nombre d'erreurs.

Les métriques de classe d'état comptent le code d'état reçu par l'appelant. Ils ne font pas la distinction entre les réponses écrites par votre application et les réponses renvoyées par Lambda. Si votre application a déjà envoyé l'état de la réponse et les en-têtes, un échec ultérieur, tel qu'un flux interrompu ou un délai d'expiration de la demande, est compté dans le code de statut d'origine. Pour identifier la source d'une erreur, utilisez l'en-tête de `lambda-web-error-type` réponse et vos journaux. Pour comptabiliser les erreurs d'application séparément, publiez vos propres statistiques. Pour plus d'informations, consultez the section called “Métriques personnalisées”.

Pour estimer le taux d'erreur d'un serveur, divisez-le `HTTPResponseStatusClass5XX` par `ExecutedRequests` sur la même période à l'aide de calculs CloudWatch métriques. Par exemple, utilisez`FILL(m5xx, 0) / m_executed`, where `m5xx` et `m_executed` are les identifiants des deux métriques. Comme il `HTTPResponseStatusClass5XX` est peu dense, utilisez-le de `FILL` telle sorte que les périodes sans erreur soient évaluées à 0 au lieu de n'avoir aucune valeur. `HTTPResponseStatusClass5XX`compte également 5xx réponses renvoyées par Lambda avant qu'une demande n'atteigne un environnement d'exécution. `ExecutedRequests`ne prend pas en compte ces réponses, de sorte que le ratio peut surestimer le taux en cas d'interruption de service.

Les métriques des demandes dans la région d'origine regroupent le trafic provenant de chaque région desservie par le point de terminaison, de sorte qu'une alarme dans la région d'origine couvre l'ensemble du point de terminaison. Créez des alarmes et des tableaux de bord à partir des valeurs de la région d'origine. Ne vous fiez pas à ces indicateurs dans d'autres régions ; voirthe section called “Télémétrie dans chaque région”.

Lambda émet des métriques de demande lorsqu'une demande est terminée. Dans le cas d'une demande de longue durée, le point de données peut apparaître jusqu'au délai imparti après le début

de la demande, de sorte que les erreurs causées par de longues demandes peuvent atteindre vos alarmes en retard. Pour le délai d'expiration de la demande, voirthe section called “Timeout”.

Métriques de l'environnement d'exécution

Les métriques de l'environnement d'exécution décrivent les ressources utilisées par les environnements d'exécution desservant votre fonction Web. Lambda les publie dans l'espace de `AWS/Lambda/Web` noms avec la `FunctionName` dimension et les centralise dans la région d'accueil de la fonction Web.

Lambda émet ces métriques une fois par minute pour chaque environnement d'exécution actif. Elles peuvent donc être rares en l'absence d'environnements d'exécution actifs. La valeur peut être 0. Un environnement d'exécution peut publier plusieurs points de données par minute, par exemple lors de son initialisation et de son arrêt. N'utilisez donc pas les `SampleCount` statistiques pour compter les environnements actifs. Pour les compter comme point de terminaison, utilisez`EndpointActiveEnvironments`.

Métrique	Unit	Statistique	Description
`EnvironmentActiveTime`	`Milliseconds`	`Sum`	Horloge murale pendant laquelle les environnements d'exécution de la fonction étaient actifs, y compris l'initialisation. Chaque point de données représente le temps d'activité d'un environnement depuis son point de données précédent, de sorte que la somme sur une période correspond au temps total consommé par l'environnement.
`EnvironmentCPUTime`	`Milliseconds`	`Sum`	Temps de vCPU consommé par les environnements d'exécution de la fonction, initialisation comprise.
`EnvironmentMaxMemoryUsage`	`Megabytes`	`Maximum`	Mémoire maximale utilisée par un environnement d'exécution jusqu'à présent au cours de sa durée de vie.

Métrique	Unit	Statistique	Description
`EnvironmentConcurrentRequests`	`Count`	`Maximum`	Le plus grand nombre de demandes traitées simultanément par un environnement d'exécution au cours de la période.
`ResponseBytes`	`Bytes`	`Sum`	Nombre d'octets de réponse envoyés par les environnements d'exécution de la fonction.

Les métriques de l'environnement d'exécution n'incluent pas `EndpointName` cette dimension. Ils couvrent tous les points de terminaison de la fonction Web.

Indicateurs régionaux d'utilisation et de limitation

Les statistiques d'utilisation et de limitation indiquent dans quelle mesure votre compte et vos terminaux sont proches de leurs limites régionales, ainsi que la limite qui a limité une demande. Le quota de taux de demandes de compte et le quota de vCPU Arm64 du compte s'appliquent séparément dans chacun Région AWS d'eux. Lambda publie donc ces métriques dans chaque région et ne les centralise pas. Pour connaître l'utilisation d'une région, consultez les statistiques de cette région. Pour les quotas, voirthe section called “Fonctions Web Lambda”.

Ces métriques sont publiées dans l'espace de `AWS/Lambda/Web/Usage` noms avec les `ExecutionRegion` dimensions `FunctionNameEndpointName`, et. Ils utilisent l'`Count`unité.

Métrique	Statistique	Quand Lambda l'émet	Description
`ExecutedRequests`	`Sum`	Uniquement pour les périodes au cours desquelles au moins une demande a atteint un environnement d'exécution dans la Région.	Le nombre de demandes qui ont atteint un environnement d'exécution dans la région.

Métrique	Statistique	Quand Lambda l'émet	Description
`EndpointActiveEnvironments`	`Maximu`	Avec des demandes adressées au point de terminaison. La valeur peut être 0. Il n'y a aucun point de données tant que le terminal ne reçoit aucune demande.	Le nombre d'environnements d'exécution actifs du point de terminaison dans la région. Comparez cette valeur avec`maxEnvironments` .
`AccountRequestThrottles`	`Sum`	clairsemé. Uniquement pendant les périodes avec au moins un tel accélérateur.	Le nombre de demandes adressées au point de terminaison qui ont été limitées parce que le compte a atteint son quota de taux de demandes dans la région.
`EndpointRequestThrottles`	`Sum`	clairsemé. Uniquement pendant les périodes avec au moins un tel accélérateur.	Le nombre de demandes qui ont été limitées parce que le point de terminaison a atteint sa limite de taux de demandes (). `rateLimit`
`AccountActiveVCPUArm64Throttles`	`Sum`	clairsemé. Uniquement pendant les périodes avec au moins un tel accélérateur.	Le nombre de demandes adressées au point de terminaison qui ont été limitées parce que leur traitement aurait dépassé le quota de vCPU Arm64 du compte dans la région. Comme les autres indicateurs d'accélération, il ne compte que les accélérateurs de ce point de terminaison. Pour voir le total du compte, additionnez-le entre les points de terminaison.

Métrique	Statistique	Quand Lambda l'émet	Description
`EndpointActiveEnvironmentThrottles`	`Sum`	clairsemé. Uniquement pendant les périodes avec au moins un tel accélérateur.	Le nombre de demandes qui ont été limitées parce que leur traitement aurait dépassé les paramètres du point de `maxEnvironments` terminaison.

Lambda attribue chaque demande limitée à une limite, de sorte qu'une demande limitée incrémente au plus une métrique d'accélération. Les requêtes que Lambda limite parce qu'un trop grand nombre d'environnements d'exécution s'initialisent en même temps renvoient le protocole HTTP 429 avec le type `Platform.EndpointConcurrentInitThrottle` d'erreur, mais n'incrémentent aucune métrique d'accélération. Les demandes limitées sont également prises en compte `HTTPResponseStatusClass4XX` dans l'espace de noms. `AWS/Lambda/Web`

Pour surveiller un `PerRegion` terminal `MultiRegion` ou un point de terminaison, consultez ou alertez sur les indicateurs d'utilisation dans chaque région, ou combinez-les dans un tableau de bord CloudWatch interrégional.

Utilisation des métriques avec d'autres CloudWatch fonctionnalités

Les `AWS/Lambda/Web` métriques étant centralisées dans la région d'origine, vous pouvez les utiliser avec les CloudWatch fonctionnalités standard de cette région, notamment :

- Amazon CloudWatch Observability Access Manager — Partagez les métriques des fonctions Web avec un compte de surveillance central afin qu'un compte puisse observer de nombreux comptes d'applications.
- Tableaux de bord et alarmes : créez des tableaux de bord et des alarmes sur les indicateurs de la région d'origine afin de couvrir l'ensemble du déploiement multirégional.

Régler une alarme sur les réponses 5xx

Créez des CloudWatch alarmes pour détecter des problèmes tels que des taux d'erreur élevés ou des ralentissements.

La commande suivante crée une alarme qui se déclenche lorsque les appelants reçoivent plus de cinq réponses 5xx du terminal sur une période de cinq minutes.

```
aws cloudwatch put-metric-alarm \
    --alarm-name my-web-app-prod-5xx \
    --namespace AWS/Lambda/Web \
    --metric-name HTTPResponseStatusClass5XX \
    --statistic Sum \
    --period 300 \
    --threshold 5 \
    --comparison-operator GreaterThanThreshold \
    --evaluation-periods 1 \
    --treat-missing-data notBreaching \
    --dimensions Name=FunctionName,Value=my-web-app Name=EndpointName,Value=prod \
    --alarm-actions arn:aws:sns:us-east-1:111122223333:my-alerts
```

Remplacez les valeurs suivantes :

- *my-web-app-prod-5xx*— Le nom de l'alarme.
- *my-web-app*— Le nom de votre fonction Web.
- *prod* : nom du point de terminaison.
- *arn:aws:sns:us-east-1:111122223333:my-alerts*— L'ARN de la rubrique Amazon SNS qui reçoit les notifications d'alarme.

`--treat-missing-data notBreaching`est important ici. `HTTPResponseStatusClass5XX`est une métrique éparse, de sorte que les périodes sans réponses 5xx ne produisent aucun point de données. Sans ce réglage, l'alarme passerait à l'`INSUFFICIENT_DATA`état pendant ces périodes.

> **Note**
>
> Les métriques des fonctions Web n'incluent pas de dimension de révision. Pour attribuer des erreurs à une révision lors d'un déploiement de Canary, définissez une variable d'environnement qui identifie la version, par exemple dans chaque révision, et incluez sa valeur dans vos journaux structurés ou en tant que dimension dans les métriques que vous publiez avec le format de métrique intégré. `APP_VERSION` Les événements du journal système, tels `revisionId` que l'enregistrement de chaque environnement d'exécution, sont `platform.initStart` également enregistrés, et l'en-tête de `lambda-web-logstream`

réponse identifie le flux de journal de l'environnement d'exécution qui a répondu à une demande. Pour la procédure de restauration, voirthe section called “Faire marche arrière”.

Journaux des fonctions Web dans Amazon CloudWatch Logs

AWS Lambda capture tout ce que votre application écrit en sortie standard et en erreur standard et l'envoie à Amazon CloudWatch Logs, avec les journaux système générés par Lambda elle-même. DansNode.js, les résultats de chaque `console` méthode, tels que`console.log`, et `console.info``console.error`, sont capturés automatiquement et filtrés en fonction du `applicationLogLevel` paramètre. Les bibliothèques de journalisation qui écrivent sur une sortie standard ou sur une erreur standard sont également capturées. Vous n'avez pas besoin d'agent de journalisation ni du SDK Amazon CloudWatch Logs.

Lambda écrit la `console` sortie sous forme d'événements de journal JSON et ajoute les `region` champs `requestIdendpointName`, et à chaque événement. Pour obtenir un exemple, consultez the section called “Rédaction de journaux structurés”.

Lambda collecte les journaux dans chaque Région AWS endroit où votre fonction Web s'exécute, puis les centralise dans la région d'origine de la fonction. Un `HomeRegion` point de terminaison s'exécute uniquement dans la région d'origine. Un `MultiRegion` point de `PerRegion` terminaison s'exécute également dans les autres régions que vous spécifiez. Lambda centralise donc les journaux de chacune de ces régions. Pour plus d’informations, consultez the section called “Types de point de terminaison”.

Groupes de journaux

Par défaut, Lambda envoie les journaux de votre fonction Web à un groupe de journaux nommé d'après la fonction :

```
/aws/lambda/web/function-name
```

Outre le groupe de journaux centralisé, Lambda utilise un groupe de journaux complémentaire pour conserver les journaux régionaux avant qu'ils ne soient centralisés. Le nom du compagnon est le nom du groupe de journaux centralisé suivi de`.local`, à la fois pour le groupe de journaux par défaut et pour un groupe de journaux personnalisé. Pour le groupe de journaux par défaut, le compagnon est :

```
/aws/lambda/web/function-name.local
```

Lambda écrit des journaux dans le groupe de `.local` journaux de chaque région où les demandes sont exécutées, y compris la région d'origine, puis les centralise dans le groupe de journaux sans le suffixe dans la région d'origine. Chaque groupe de `.local` journaux contient uniquement les journaux de sa propre région. Lambda ne supprime pas les événements du groupe de `.local` journaux après la centralisation. Le paramètre de conservation du groupe de journaux détermine sa durée de conservation.

Les groupes de journaux n'existent pas tant que votre fonction Web n'a pas répondu à sa première demande. Le groupe de journaux centralisé de la région d'origine peut apparaître après le groupe de `.local` journaux. Pour le calendrier de centralisation, voirthe section called “Latence de centralisation”.

Lambda crée le groupe de journaux par défaut et chaque `.local` groupe de CloudWatch journaux avec les paramètres Amazon Logs par défaut, de sorte que leurs événements n'expirent jamais, sauf si vous définissez une politique de rétention. Vous pouvez modifier leur politique de rétention, de chiffrement et de ressources une fois que Lambda les a créés. Définissez-les sur le groupe de `.local` journaux de chaque région où s'exécute le point de terminaison et sur le groupe de journaux centralisé de la région d'origine.

Comme le groupe de `.local` journaux n'attend pas la centralisation, il est utile pour résoudre un problème dans une région spécifique. Le groupe de journaux centralisé contient les journaux de chaque région. Créez donc des requêtes partagées, des filtres d'abonnement, des filtres métriques et une automatisation qui doivent couvrir l'ensemble de l'application dans le groupe de journaux centralisé. Pour connaître le comportement de la télémétrie dans chaque région, voir. the section called “Télémétrie dans chaque région”

Utilisation d'un groupe de journaux personnalisé

Vous pouvez envoyer les journaux de votre fonction Web à un groupe de journaux que vous choisissez à la place du groupe par défaut. Utilisez un groupe de journaux personnalisé lorsque vous souhaitez mettre en place des politiques de rétention, de chiffrement ou de ressources avant l'arrivée du premier événement de journal. Un groupe de journaux personnalisé vous permet également de regrouper les journaux de plusieurs fonctions. Pour appliquer ces paramètres dès le départ, créez vous-même le groupe de journaux et son `.local` compagnon avant d'acheminer le trafic vers la révision. Si l'un des groupes de journaux n'existe pas, Lambda le crée lors de la première utilisation avec les paramètres par défaut, et vous pouvez mettre à jour ses paramètres par la suite. Lambda

ne peut créer un groupe de journaux que si le rôle d'exécution est autorisé à créer des groupes de journaux. Pour les autorisations requises, consultez the section called “Rôle d'exécution”.

Pour envoyer des journaux à un groupe de journaux personnalisé (AWS CLI)

1. Dans la région d'origine, créez le groupe de journaux et son `.local` compagnon, puis définissez la durée de conservation que vous souhaitez pour chacun d'eux. Pour un point de `PerRegion` terminaison `MultiRegion` ou un point de terminaison, créez également le groupe de `.local` journaux dans chaque autre région desservie par le point de terminaison, en exécutant `.local` les commandes `--region` définies sur cette région.

```
aws logs create-log-group --log-group-name /my-app/web-logs
aws logs create-log-group --log-group-name /my-app/web-logs.local

aws logs put-retention-policy \
    --log-group-name /my-app/web-logs \
    --retention-in-days 30

aws logs put-retention-policy \
    --log-group-name /my-app/web-logs.local \
    --retention-in-days 30
```

2. Créez une révision qui spécifie le groupe de journaux dans la `telemetryConfig` section `deserviceConfig`.

```
aws lambda-web create-web-function-revision \
    --function-name my-web-app \
    --build-config '{
      "codeConfig": {
        "s3Object": { "bucket": "my-bucket", "key": "my-app.zip" }
      },
      "runtimeConfig": { "runtime": "nodejs24.x" }
    }' \
    --service-config '{
      "executionRoleArn": "arn:aws:iam::111122223333:role/my-web-function-role",
      "telemetryConfig": {
        "loggingConfig": {
          "logGroup": "/my-app/web-logs"
        }
      }
    }'
```

3. Acheminez le trafic vers la nouvelle révision. Pour plus d'informations, consultez the section called "Modèles de déploiement".

Comme la configuration de journalisation fait partie de la révision, elle est immuable pour cette révision. Pour modifier le groupe de journaux ultérieurement, créez une autre révision. Pour plus d'informations, consultez the section called "Révisions".

Contrôles de journalisation

La `loggingConfig` section contrôle la destination et la sévérité minimale des journaux. Ces paramètres font partie de la révision.

Paramètre	Valeurs	Par défaut	Description
`logGroup`	Nom du groupe de journaux	`/aws/lambda/web/`*`function-name`*	Le groupe de CloudWatch journaux Amazon Logs qui reçoit vos journaux.
`applicationLogLevel`	`TRACE` | `DEBUG` | `INFO` | `WARN` | `ERROR` | `FATAL`	`INFO`	La sévérité minimale des journaux de votre application que Lambda envoie à Amazon CloudWatch Logs. Les journaux inférieurs à ce niveau sont supprimés. Node.jsn'a pas de méthode `FATAL` console, donc un niveau de `FATAL` se comporte commeERROR.
`systemLogLevel`	`DEBUG` | `INFO` | `WARN`	`INFO`	La sévérité minimale des journaux Lambda-generated système que Lambda envoie à Amazon CloudWatch Logs. Pour le niveau de chaque événement système, voirthe section called "Journaux du système".

L'exemple suivant crée une révision qui supprime les journaux d'application ci-dessous `WARN` :

```
aws lambda-web create-web-function-revision \
    --function-name my-web-app \
    --build-config '{
      "codeConfig": {
        "s3Object": { "bucket": "my-bucket", "key": "my-app.zip" }
      },
      "runtimeConfig": { "runtime": "nodejs24.x" }
    }' \
    --service-config '{
      "executionRoleArn": "arn:aws:iam::111122223333:role/my-web-function-role",
      "telemetryConfig": {
        "loggingConfig": {
          "applicationLogLevel": "WARN",
          "systemLogLevel": "INFO"
        }
      }
    }'
```

L'`applicationLogLevel`augmentation de la production réduit à la fois le volume des grumes et les coûts. Réduisez-le temporairement à `DEBUG` ou `TRACE` lorsque vous étudiez un problème.

Journaux du système

Outre les résultats de votre application, votre groupe de journaux reçoit les journaux système générés par Lambda concernant le cycle de vie de l'environnement d'exécution, tels que l'initialisation et l'arrêt de l'environnement. `systemLogLevel`À utiliser pour contrôler la quantité de cette Lambda émise.

Les journaux système sont utiles pour corréler le comportement des applications avec les événements de plate-forme. Par exemple, un pic de latence correspondant à l'initialisation de l'environnement indique un démarrage à froid plutôt que le code de votre application. Pour le cycle de vie décrit par ces journaux, voirthe section called “Cycle de vie environnemental”.

Les fonctions Web émettent les événements système suivants. Réglez `systemLogLevel` le niveau le plus bas dont vous avez besoin. Par exemple, configurez-le pour qu'il reçoive `platform.requestComplete` ou `DEBUG` pour qu'il ne reçoive que `WARN` les avertissements d'échec et de perte de journal.

Type d’événement	Niveau	Remarques
`platform.initStart`	`INFO`	Aucune
`platform.initReport`	`INFO`sur le succès, `WARN` sur l'échec	Un échec indique une erreur d'initialisation, telle qu'une erreur lors de l'importation de votre code.
`platform.invokeStart`	`INFO`	Aucune
`platform.requestComplete`	`DEBUG`	Émis une fois pour chaque requête HTTP, y compris les demandes ayant échoué. Comme il s'agit d'un volume élevé, il n'est pas émis au niveau du journal système par défaut.
`platform.invokeSummary`	`INFO`	Périodique. Émis toutes les 60 secondes environ pour chaque environnement d'exécution actif.
`platform.invokeReport`	`INFO`sur le succès, `WARN` sur l'échec	
`platform.spinDownStart`	`INFO`	
`platform.spinDownReport`	`INFO`sur le succès, `WARN` sur l'échec	Un échec indique que votre application ne s'est pas fermée dans la seconde suivant la réception `SIGTERM` (`Runtime.SpinDownTimeout`) ou qu'elle s'est terminée avec une erreur (`Runtime.ExitError`).
`platform.logsDropped`	`WARN`	Indique que Lambda a supprimé les événements du journal.

Pour les champs de chaque événement système, voirthe section called “Schéma du journal système”.

L'en-tête de `lambda-web-request-id` réponse identifie la demande et l'en-tête de `lambda-web-logstream` réponse identifie le flux de journal de l'environnement qui l'a traitée. Utilisez ces valeurs pour corréler la réponse d'un client avec les journaux de l'application et du système. Pour plus d’informations, consultez the section called “En-têtes de réponse”.

Pour rechercher les événements du flux de journal identifié dans le groupe de journaux centralisé de la région d'origine, filtrez par le nom du flux en tant que préfixe. Vous pouvez également lire le flux par son nom exact dans le groupe de `.local` journaux de la région qui a répondu à la demande.

```
aws logs filter-log-events \
    --log-group-name /aws/lambda/web/my-web-app \
    --log-stream-name-prefix "LAMBDA_WEB_LOGSTREAM" \
    --region us-east-1
```

Pour suivre les journaux récents tout en reproduisant un problème, utilisez :

```
aws logs tail /aws/lambda/web/my-web-app \
    --follow \
    --region us-east-1
```

Rédaction de journaux structurés

Passez un objet à une `console` méthode afin que Lambda l'écrive sous forme d'objet JSON dans le `message` champ. Vous pouvez ensuite interroger des champs individuels dans Amazon CloudWatch Logs Insights plutôt que de les faire correspondre sur des sous-chaînes. Ne transmettez pas une chaîne avec laquelle vous avez créé`JSON.stringify`. Lambda écrit une chaîne sous forme de valeur de chaîne échappée, de sorte que ses champs ne peuvent pas être interrogés.

```
function logRequest(req, statusCode, durationMs) {
  console.info({
    method: req.method,
    path: req.url,
    statusCode: statusCode,
    durationMs: durationMs
  });
}
```

Lambda écrit un événement de journal similaire au suivant :

```
{
  "timestamp": "2026-09-25T11:29:02.711Z",
  "level": "INFO",
  "message": {
    "method": "GET",
    "path": "/hello-world",
    "statusCode": 200,
    "durationMs": 100
  },
  "requestId": "US3NHLM77IRXDFLBADYHGIZZNM",
  "endpointName": "prod",
  "region": "us-east-1"
}
```

Vous pouvez ensuite interroger les champs directement. Par exemple, la requête Amazon CloudWatch Logs Insights suivante renvoie les 20 demandes les plus récentes ayant renvoyé un statut 5xx :

```
fields @timestamp, message.method, message.path, message.statusCode, message.durationMs
| filter message.statusCode >= 500
| sort @timestamp desc
| limit 20
```

Pour publier des métriques personnalisées à partir de vos journaux au lieu de simplement les interroger, utilisez le format de métrique intégré. Pour plus d'informations, consultez the section called "Métriques personnalisées".

Utilisation des fonctionnalités d'Amazon CloudWatch Logs avec vos journaux

Les journaux étant centralisés dans la région d'origine, vous pouvez utiliser les fonctionnalités standard d'Amazon CloudWatch Logs dans cette région, notamment :

- Live Tail — Diffusez les événements du journal au fur et à mesure qu'ils arrivent pendant que vous reproduisez un problème. Les événements atteignent le groupe de journaux centralisé après la centralisation. Par conséquent, dans les plus brefs délais, exécutez Live Tail sur le groupe de `.local` journaux de la région qui répond à vos demandes.
- Logs Insights : champs de requête dans vos événements de journal JSON.

- Centralisation des journaux : transférez vos journaux vers un autre compte ou une autre destination à l'aide des fonctionnalités de centralisation d'Amazon CloudWatch Logs, si vous regroupez des journaux en dehors du compte de la fonction.
- Filtres d'abonnement et filtres métriques : déclenchez le traitement en aval ou déduisez des métriques à partir de modèles de journalisation.

Appliquez les fonctionnalités qui doivent couvrir l'ensemble de l'application au groupe de journaux centralisé de la région d'origine. Un groupe de `.local` journaux ne contient que les journaux de sa propre région. Pour plus d'informations, consultez the section called “Télémétrie dans chaque région”.

Schéma des événements du journal système pour Lambda Web Functions

Lambda écrit les événements système suivants dans le groupe de journaux de votre fonction Web. Chaque événement est un objet JSON avec les champs d'enveloppe décrits dans the section called “Enveloppe d'événement” et un `record` objet dont les champs dépendent du type d'événement. Le niveau de chaque événement détermine si Lambda le diffuse. Pour plus d’informations, consultez the section called “Journaux du système”.

Type d’événement	Objet d'enregistrement	Description
`platform.initStart`	`PlatformInitStart`	L'initialisation de l'environnement a commencé.
`platform.initReport`	`PlatformInitReport`	Rapport sur l'initialisation de l'environnement, indiquant si elle a réussi ou échoué.
`platform.invokeStart`	`PlatformInvokeStart`	L'environnement a commencé à répondre aux demandes.
`platform.requestComplete`	`PlatformRequestComplete`	Une requête HTTP terminée. Connecté uniquement à DEBUG.
`platform.invokeSummary`	`PlatformInvokeSummary`	Résumé de l'activité de l'environnement, émis toutes les 60 secondes environ.

Type d'événement	Objet d'enregistrement	Description
`platform.invokeReport`	`PlatformInvokeReport`	Rapport sur l'ensemble de la période de service de l'environnement, émis lorsqu'il cesse de servir.
`platform.spinDownStart`	`PlatformSpinDownStart`	L'arrêt de l'environnement a commencé.
`platform.spinDownReport`	`PlatformSpinDownReport`	Rapport d'arrêt de l'environnement.
`platform.logsDropped`	`PlatformLogsDropped`	Les enregistrements de journaux ont été supprimés car les journaux étaient produits plus rapidement qu'ils ne pouvaient être livrés.

Dans les listes de champs de cette page, un point d'interrogation (?) après le nom d'un champ signifie que le champ n'est peut-être pas présent. Les types qui ne sont pas des types JSON `InitTypeStatus`, tels que`InvokeSummaryMetrics`, ou, sont définis dansthe section called "Types d'objets partagés", et chacun est lié à sa définition.

`Platform.initStart`

La phase d'initialisation de l'environnement a débuté.

Niveau : `INFO`

L'objet `record` comporte les champs suivants :

- `functionName`(`String`) — Nom de la fonction.
- `revisionId`(`String`) — La révision exécutée par l'environnement.
- `instanceId`(`String`) — Identifiant de l'environnement d'exécution.
- `initializationType`(`InitType`) — Comment Lambda a initialisé l'environnement.
- `runtimeVersion`(`String`) — Version d'exécution exécutée par l'environnement.
- `runtimeVersionArn`(`String`) — Le nom de ressource Amazon (ARN) de la version d'exécution.

```
{
  "timestamp": "2026-09-25T11:12:30.893Z",
  "level": "INFO",
  "type": "platform.initStart",
  "region": "us-east-1",
  "record": {
    "runtimeVersion": "nodejs24.x:nodejs.web24.v51",
    "runtimeVersionArn": "arn:aws:lambda:us-east-1::runtime/nodejs24.x/version/
nodejs.web24.v51",
    "functionName": "my-web-app",
    "revisionId": "rev-fs0fq",
    "instanceId": "52754708-44f1-407a-a1fd-6d2a98175a45",
    "initializationType": "native-http"
  }
}
```

`Rapport Platform.init`

Rapport global de la phase d'initialisation.

Niveau : `INFO` lorsque le statut est un succès, en `WARN` cas d'échec.

L'objet `record` comporte les champs suivants :

- `status`(`Status`) — Résultat de la phase d'initialisation.
- `errorType?`(`String`) — Présent lorsque le statut est un échec. Des valeurs telles que `Runtime.ImportCodeErrorApplication.InitCodeError`, et`Runtime.InitTimeout`.
- `initializationType`(`InitType`) — Comment Lambda a initialisé l'environnement.
- `metrics`(`InitReportMetrics`) — Métriques pour la phase d'initialisation.

Exemple de réussite :

```
{
  "timestamp": "2026-09-25T11:12:31.143Z",
  "level": "INFO",
  "type": "platform.initReport",
  "region": "us-east-1",
  "record": {
    "status": "success",
    "initializationType": "native-http",
    "metrics": {
```

```
      "totalDurationMs": 304.000,
      "totalCpuTimeMs": 143.000,
      "maxMemoryUsageMb": 142
    }
  }
}
```

Exemple d'échec, lorsque le module de gestion n'a pas pu être chargé :

```
{
  "timestamp": "2026-09-25T11:16:04.164Z",
  "level": "WARN",
  "type": "platform.initReport",
  "region": "us-east-1",
  "record": {
    "status": "failure",
    "errorType": "Runtime.ImportCodeError",
    "initializationType": "native-http",
    "metrics": {
      "totalDurationMs": 320.000,
      "totalCpuTimeMs": 137.000,
      "maxMemoryUsageMb": 138
    }
  }
}
```

`Platform.invokeStart`

L'environnement a terminé son initialisation et a commencé à traiter les demandes. Lambda émet cet événement une fois par environnement, et non une fois par requête, et uniquement lorsque l'initialisation a réussi.

Niveau : `INFO`

L'objet `record` comporte les champs suivants :

- `functionName`(`String`) — Nom de la fonction.
- `revisionId`(`String`) — La révision exécutée par l'environnement.
- `instanceId`(`String`) — Identifiant de l'environnement d'exécution.

```
{
```

```
  "timestamp": "2026-09-25T11:12:31.144Z",
  "level": "INFO",
  "type": "platform.invokeStart",
  "region": "us-east-1",
  "record": {
    "functionName": "my-web-app",
    "revisionId": "rev-fs0fq",
    "instanceId": "52754708-44f1-407a-a1fd-6d2a98175a45"
  }
}
```

`Plateforme. Demande terminée`

Une requête HTTP s'est terminée, avec succès ou non.

Niveau :`DEBUG`, donc Lambda ne le livre que lorsqu'`systemLogLevel`il est. `DEBUG`

L'objet `record` comporte les champs suivants :

- `requestId`(`String`) — L'ID de la demande.
- `endpointName`(`String`) — Le point de terminaison qui a répondu à la demande.
- `result`(`Integer`) — Le code d'état HTTP a été renvoyé au client.
- `errorType?`(`String`) — Présent lorsque Lambda a échoué à la demande. Des valeurs telles que `Runtime.RequestTimeout` et`Platform.InvalidRequest`.
- `metrics`([RequestCompleteMetrics](#)) — Métriques de la demande.

Exemple de réussite :

```
{
  "timestamp": "2026-09-25T11:12:31.154Z",
  "level": "DEBUG",
  "type": "platform.requestComplete",
  "region": "us-east-1",
  "record": {
    "requestId": "KXH25FBDZ33GP4TQ4ARAUYSTSA",
    "endpointName": "default",
    "result": 200,
    "metrics": {
      "durationMs": 4.484,
      "responseBytes": 40
```

```
    }
  }
}
```

Exemple de délai d'attente :

```
{
  "timestamp": "2026-09-25T11:12:34.926Z",
  "level": "DEBUG",
  "type": "platform.requestComplete",
  "region": "us-east-1",
  "record": {
    "requestId": "5SXHGVX2GD64ND6NQVEBAY235Q",
    "endpointName": "default",
    "result": 504,
    "errorType": "Runtime.RequestTimeout",
    "metrics": {
      "durationMs": 3001.229,
      "responseBytes": 0
    }
  }
}
```

`Résumé de Platform.invoke`

Résume une fenêtre d'environ 60 secondes d'activité d'un environnement. Lambda l'émet pour tous les environnements actifs, y compris les fenêtres inactives où `requests` la valeur est 0.

Niveau : `INFO`

L'objet `record` comporte les champs suivants :

- `startTime`(`String`) — Début de la fenêtre de résumé (RFC 3339).
- `instanceId`(`String`) — Identifiant de l'environnement d'exécution.
- `metrics`(`InvokeSummaryMetrics`) — Mesures pour la fenêtre.

```
{
  "timestamp": "2026-09-25T11:13:31.143Z",
  "level": "INFO",
  "type": "platform.invokeSummary",
  "region": "us-east-1",
```

```
  "record": {
    "startTime": "2026-09-25T11:12:31.144547426Z",
    "instanceId": "52754708-44f1-407a-a1fd-6d2a98175a45",
    "metrics": {
      "requests": 4,
      "concurrentRequests": 1,
      "cpuTimeMs": 420.000,
      "maxMemoryUsageMb": 154
    }
  }
}
```

`Rapport Platform.InvokeReport`

Rapport global de la période de service de l'environnement, depuis InvokeStart jusqu'à l'arrêt du service. Lambda l'émet une fois par environnement, à l'arrêt.

Niveau : `INFO` lorsque le statut est un succès, en `WARN` cas d'échec.

L'objet `record` comporte les champs suivants :

- `status`(`Status`) — Le résultat de la période de service.
- `errorType?`(`String`) — Présent lorsque le statut est un échec. Des valeurs telles que `Runtime.ExitRuntime.ExitError`, et`Runtime.OutOfMemory`.
- `instanceId`(`String`) — Identifiant de l'environnement d'exécution.
- `metrics`(`InvokeReportMetrics`) — Indicateurs relatifs à la période de service.

Le délai d'expiration d'une demande ne correspond pas à la période de service. Les `status` séjourssuccess.

Exemple de réussite :

```
{
  "timestamp": "2026-09-25T11:19:11.858Z",
  "level": "INFO",
  "type": "platform.invokeReport",
  "region": "us-east-1",
  "record": {
    "status": "success",
    "instanceId": "52754708-44f1-407a-a1fd-6d2a98175a45",
```

```
    "metrics": {
      "totalCpuTimeMs": 973.000,
      "totalDurationMs": 400723.000,
      "totalRequests": 4,
      "concurrentRequests": 1,
      "maxMemoryUsageMb": 157
    }
  }
}
```

Exemple d'échec :

```
{
  "timestamp": "2026-09-25T11:19:11.858Z",
  "level": "WARN",
  "type": "platform.invokeReport",
  "region": "us-east-1",
  "record": {
    "status": "failure",
    "errorType": "Runtime.OutOfMemory",
    "instanceId": "52754708-44f1-407a-a1fd-6d2a98175a45",
    "metrics": {
      "totalCpuTimeMs": 973.000,
      "totalDurationMs": 400723.000,
      "totalRequests": 4,
      "concurrentRequests": 1,
      "maxMemoryUsageMb": 512
    }
  }
}
```

`platform.spin DownStart`

L'arrêt de l'environnement a commencé.

Niveau : `INFO`

L'objet `record` comporte les champs suivants :

- `functionName`(`String`) — Nom de la fonction.
- `revisionId`(`String`) — La révision exécutée par l'environnement.
- `instanceId`(`String`) — Identifiant de l'environnement d'exécution.

```
{
  "timestamp": "2026-09-25T11:19:11.858Z",
  "level": "INFO",
  "type": "platform.spinDownStart",
  "region": "us-east-1",
  "record": {
    "functionName": "my-web-app",
    "revisionId": "rev-fs0fq",
    "instanceId": "52754708-44f1-407a-a1fd-6d2a98175a45"
  }
}
```

`platform.spin DownReport`

Rapport global de la fermeture.

Lambda envoie un message `SIGTERM` à votre application et attend jusqu'à 1 seconde pour qu'elle se ferme. Si l'application est toujours en cours d'exécution, Lambda l'arrête `SIGKILL` et signale un échec du type d'erreur. `Runtime.SpinDownTimeout`

Niveau : `INFO` lorsque le statut est un succès, en `WARN` cas d'échec.

L'objet `record` comporte les champs suivants :

- `status`(`Status`) — Le résultat de la phase d'arrêt.
- `errorType?`(`String`) — Présent lorsque le statut est un échec. Des valeurs telles que `Runtime.SpinDownTimeout` et`Runtime.ExitError`.
- `metrics`(`SpinDownReportMetrics`) — Métriques relatives à la phase d'arrêt.

Exemple de réussite :

```
{
  "timestamp": "2026-09-25T11:19:11.879Z",
  "level": "INFO",
  "type": "platform.spinDownReport",
  "region": "us-east-1",
  "record": {
    "status": "success",
    "metrics": {
      "totalDurationMs": 21.000,
      "totalCpuTimeMs": 8.000,
```

```
      "maxMemoryUsageMb": 157
    }
  }
}
```

Exemple d'échec :

```
{
  "timestamp": "2026-09-25T11:19:12.879Z",
  "level": "WARN",
  "type": "platform.spinDownReport",
  "region": "us-east-1",
  "record": {
    "status": "failure",
    "errorType": "Runtime.SpinDownTimeout",
    "metrics": {
      "totalDurationMs": 1021.000,
      "totalCpuTimeMs": 8.000,
      "maxMemoryUsageMb": 157
    }
  }
}
```

`Plate-forme. LogsDropped`

Les enregistrements de journaux ont été supprimés car les journaux étaient produits plus rapidement qu'ils ne pouvaient être livrés.

Niveau : `WARN`

L'objet `record` comporte les champs suivants :

- `reason`(`String`) — Pourquoi les records ont été supprimés.
- `droppedRecords`(`Integer`) — Enregistrements perdus depuis le dernier enregistrement livré.
- `droppedBytes`(`Integer`) — Octets perdus depuis le dernier enregistrement livré.

Les deux comptes s'accumulent au fil des baisses consécutives et sont remis à 0 après la délivrance d'un record.

```
{
  "timestamp": "2026-09-25T11:20:00.000Z",
```

```
  "level": "WARN",
  "type": "platform.logsDropped",
  "region": "us-east-1",
  "record": {
    "reason": "Some logs were dropped because the downstream consumer is slower than
 the logs production rate",
    "droppedRecords": 120,
    "droppedBytes": 48000
  }
}
```

Types d'objets partagés

Les types suivants apparaissent dans les listes de champs des événements de cette page.

Enveloppe d'événement

Chaque événement système comporte les champs d'enveloppe suivants :

- `timestamp`(`String`) — RFC 3339 en UTC.
- `level`(`Level`) — Le niveau de l'événement.
- `type`(`String`) — Type d'événement (`platform.*`).
- `region`(`String`) — Région dans laquelle s'exécutait l'environnement d'exécution.
- `record`(`Object`) — Les champs spécifiques à l'événement.

`InitType`

Chaîne enum qui décrit comment Lambda a initialisé l'environnement. Les fonctions Web sont toujours utiliséesnative-http.

`Niveau`

Chaîne enum pour le niveau d'un événement système : `DEBUG`INFO, ou`WARN`. Les événements du système ne sont jamais `ERROR` ou`FATAL`. Les événements du rapport `INFO` indiquent que le statut est `WARN` un succès ou un échec.

`Statut`

Chaîne enum qui décrit le résultat d'une phase : `success` ou`failure`. Quand c'est le cas`failure`, l'enregistrement contient également`errorType`.

`InitReportMetrics`

- `totalDurationMs`(`Double`) — Wall-clock heure de la phase d'initialisation.
- `totalCpuTimeMs`(`Double`) : temps processeur consommé lors de l'initialisation.
- `maxMemoryUsageMb`(`Integer`) — Mémoire maximale de l'environnement, en MiB.

`RequestCompleteMetrics`

- `durationMs`(`Double`) — Wall-clock heure de la demande.
- `responseBytes`(`Integer`) — Octets du corps de réponse envoyés.

`InvokeSummaryMetrics`

- `requests`(`Integer`) — Demandes terminées dans la fenêtre.
- `concurrentRequests`(`Integer`) — Nombre maximal de demandes simultanées dans la fenêtre.
- `cpuTimeMs`(`Double`) : temps processeur consommé dans la fenêtre.
- `maxMemoryUsageMb`(`Integer`) — Mémoire maximale de l'environnement, en MiB.

`InvokeReportMetrics`

- `totalCpuTimeMs`(`Double`) : temps passé par le processeur pendant la période de service.
- `totalDurationMs`(`Double`) : Wall-clock temps écoulé entre InvokeStart et l'arrêt du service par l'environnement.
- `totalRequests`(`Integer`) — Nombre total de demandes traitées.
- `concurrentRequests`(`Integer`) — Nombre maximal de demandes simultanées au cours de la période.
- `maxMemoryUsageMb`(`Integer`) — Mémoire maximale de l'environnement, en MiB.

`SpinDownReportMetrics`

- `totalDurationMs`(`Double`) — Wall-clock heure de la phase d'arrêt.
- `totalCpuTimeMs`(`Double`) : temps du processeur consommé lors de l'arrêt.
- `maxMemoryUsageMb`(`Integer`) — Mémoire maximale de l'environnement, en MiB.

Publication de métriques personnalisées avec le format de métrique intégré

Avec le format de métrique CloudWatch intégré (EMF) d'Amazon, vous pouvez publier vos propres statistiques à partir de AWS Lambda Web Functions, telles que les commandes passées, le taux de réussite du cache ou le temps de latence des paiements. Votre application écrit un objet JSON structuré dans ses journaux et en CloudWatch extrait les métriques. Utilisez des métriques personnalisées pour suivre les activités de votre application. Les métriques publiées par Lambda décrivent uniquement les résultats des demandes et l'utilisation des ressources.

Vous pouvez également publier des métriques personnalisées en appelant directement l' CloudWatch `PutMetricData`API, mais nous recommandons EMF pour les fonctions Web :

- Aucune latence de requête supplémentaire : votre application n'appelle pas l' CloudWatch API sur le chemin qui sert votre réponse HTTP.
- Aucune autorisation supplémentaire — Vous n'avez pas besoin d'`cloudwatch:PutMetricData`autorisation. EMF utilise les mêmes autorisations Amazon CloudWatch Logs dont le rôle d'exécution a déjà besoin pour les journaux.
- Centralisation avec vos journaux : comme les métriques EMF voyagent avec vos journaux, la région d'origine possède les valeurs de chaque région desservie par le terminal. Les métriques que vous utilisez pour publier `PutMetricData` apparaissent uniquement dans la région dans laquelle vous les appelez.

Comment EMF fonctionne avec les fonctions Web

Les métriques EMF sont transmises de votre application aux CloudWatch étapes suivantes :

1. Votre application écrit un objet EMF-formatted JSON, suivi d'une nouvelle ligne, directement sur la sortie standard.
2. Lambda le capture sous forme d'événement de journal dans la région où la demande a été exécutée et le centralise dans le home Région AWS, comme toute autre sortie de journal. Pour plus de détails, consultez the section called “Journaux”.
3. CloudWatch extrait les métriques de l'objet dans la région où la demande a été exécutée, et Lambda réplique les métriques dans la région d'origine. Les métriques apparaissent dans l'espace de noms que vous spécifiez dans l'objet. Dans la région d'origine, les métriques incluent les valeurs de chaque région desservie par le point de terminaison.

Vos métriques personnalisées apparaissent dans votre propre espace de noms, pas dans`AWS/Lambda/Web`. Cet espace de noms est réservé aux métriques publiées par Lambda.

Publication d'une métrique personnalisée

L'Node.jsexemple suivant publie une `CheckoutLatency` métrique et une `OrdersPlaced` métrique sous l'espace de `MyWebApp` noms, avec une `PaymentProvider` dimension. Il écrit l'objet EMF avec`process.stdout.write`. Ne transmettez pas d'objet EMF à une `console` méthode. Lambda encapsule la `console` sortie dans son propre journal d'événements JSON et n'extrait CloudWatch pas les métriques de l'objet encapsulé.

```
function publishCheckoutMetrics(provider, latencyMs, orders) {
  process.stdout.write(JSON.stringify({
    _aws: {
      Timestamp: Date.now(),
      CloudWatchMetrics: [
        {
          Namespace: 'MyWebApp',
          Dimensions: [['PaymentProvider']],
          Metrics: [
            { Name: 'CheckoutLatency', Unit: 'Milliseconds' },
            { Name: 'OrdersPlaced', Unit: 'Count' }
          ]
        }
      ]
    },
    PaymentProvider: provider,
    CheckoutLatency: latencyMs,
    OrdersPlaced: orders,
    // Fields outside the metric definitions are kept as searchable log context.
    requestPath: '/checkout'
  }) + '\n');
}
```

Au lieu de créer vous-même des objets EMF, vous pouvez utiliser une bibliothèque cliente EMF, telle que aws-embedded-metrics pour le site Web. Node.js GitHub Pour obtenir la liste des bibliothèques, consultez la section Création de journaux au format métrique intégré à l'aide des bibliothèques clientes dans le guide de CloudWatch l'utilisateur Amazon. Avant de vous fier à une bibliothèque, vérifiez qu'elle écrit les objets EMF directement sur la sortie standard d'une fonction Web, plutôt que par le biais `console` ou vers un CloudWatch agent.

Notez les trois rôles que jouent les champs dans un objet EMF :

- Les champs nommés dans `Metrics` deviennent CloudWatch des métriques.
- Les champs nommés dans `Dimensions` deviennent des dimensions métriques. Maintenez le nombre de valeurs de dimension distinctes à un faible niveau. Chaque combinaison crée une métrique distincte.
- Tout autre champ est conservé dans le journal des événements en tant que contexte que vous pouvez interroger avec Amazon CloudWatch Logs Insights, mais ne crée pas de métrique.

Utilisez délibérément la dernière propriété : associez des valeurs de cardinalité élevée, telles qu'un numéro de demande ou un numéro de client, sous forme de champs simples plutôt que sous forme de dimensions, afin de pouvoir trouver la demande spécifique dans Logs Insights sans multiplier le nombre de métriques.

Facturation pour des mesures personnalisées

L'EMF génère à la fois l'ingestion de logs et des frais métriques personnalisés. L'événement du journal est facturé aux prix d'Amazon CloudWatch Logs, et les métriques extraites sont facturées en tant que métriques CloudWatch personnalisées. La première centralisation d'un événement de journal est gratuite. CloudWatch extrait les métriques EMF dans la région où la demande a été exécutée, et Lambda les réplique dans la région d'origine, de sorte qu'une demande traitée en dehors de la région d'origine produit des métriques personnalisées dans les deux régions.

Le volume du journal, le nombre de mesures et le nombre de combinaisons de dimensions distinctes ont une incidence sur les coûts. Publiez les métriques à la granularité sur laquelle vous souhaitez émettre une alarme ou sur un graphique, et évitez les dimensions à cardinalité élevée.

Pour les prix actuels, consultez les CloudWatchtarifs Amazon.

Journalisation des appels d'API de fonction Web à l'aide de AWS CloudTrail

Avec AWS CloudTrail, vous pouvez suivre les actions entreprises par un utilisateur, un rôle ou Service AWS dans les fonctions AWS Lambda Web. CloudTrail fournit un enregistrement de ces actions. CloudTrail capture les invocations de fonctions Web sous forme d'événements de données. Vous pouvez utiliser ces informations pour déterminer qui a invoqué une fonction Web, quand et d'où, ce qui facilite l'analyse de sécurité et l'audit opérationnel.

Événements de données de fonction Web dans CloudTrail

Les événements de données fournissent des informations sur les opérations effectuées sur une ressource. Par exemple, l'appel d'un point de terminaison de fonction Web est un événement de données. Ces opérations sont également connues sous le nom d'opérations de plan de données, et elles portent souvent sur un volume élevé. Par défaut, CloudTrail n'enregistre pas les événements liés aux données et l'historique des CloudTrail événements ne les enregistre pas.

Des frais supplémentaires sont facturés pour les événements de données. Pour en savoir plus, consultez Tarification de CloudTrail .

Vous pouvez enregistrer les événements de données pour le type de `AWS::Lambda::WebFunction` ressource à l'aide de la CloudTrail console ou AWS CLI des opérations de CloudTrail l'API. CloudTrail enregistre chaque invocation dans la région Région AWS qui a répondu à la demande et `awsRegion` identifie cette région. Contrairement aux journaux et aux métriques, les événements d'invocation ne sont pas centralisés dans la région d'origine. Pour un point de `PerRegion` terminaison `MultiRegion` ou un point de terminaison, utilisez un magasin de données de suivi ou d'événement multirégional afin que les appels soient enregistrés dans chaque région desservie par le point de terminaison.

Le tableau suivant indique le type d'événement de données pour les fonctions Web.

Type d'événement de données (console)	valeur resources.type	API de données connectées à CloudTrail
Fonction Web Lambda	`AWS::Lambda::WebFunction`	`InvokeWebFunctionEndpoint`

CloudTrail enregistre les identificateurs clés suivants pour une invocation de fonction Web :

Identifiant	Value
`eventSource`	`lambda.amazonaws.com`
`eventName`	`InvokeWebFunctionEndpoint` . Il s'agit de la valeur sur laquelle filtrer.
Action IAM	`lambda:InvokeWebFunctionEndpoint`

Identifiant	Value
`readOnly`	`false`, car un appel exécute votre code de fonction.
`resources.type`	`AWS::Lambda::WebFunction`
`resources.ARN`	L'ARN de la fonction, et non l'ARN du point de terminaison. Les sélecteurs de parcours fonctionnent donc au niveau de la fonction.

Le sélecteur d'événements avancé suivant enregistre les appels pour une seule fonction Web.

```
[
    {
        "Name": "web-function-invokes",
        "FieldSelectors": [
            { "Field": "eventCategory", "Equals": ["Data"] },
            { "Field": "resources.type", "Equals": ["AWS::Lambda::WebFunction"] },
            { "Field": "resources.ARN", "Equals": ["arn:aws:lambda:us-
east-1:111122223333:web-function/hello-world"] }
        ]
    }
]
```

Pour activer les événements de données sur un parcours, procédez comme suit.

Pour activer et vérifier les événements relatifs aux données de la fonction Web (AWS CLI)

1. Créez ou choisissez le parcours qui enregistrera les événements liés aux données. Pour obtenir des instructions, consultez la section Journalisation des événements liés aux données dans le guide de AWS CloudTrail l'utilisateur.
2. Enregistrez le sélecteur d'événements avancé suivant sous`web-function-data-events.json`. Il enregistre les appels pour une fonction Web. Pour enregistrer les appels pour chaque fonction Web du compte, supprimez le sélecteur de `resources.ARN` champs.

   ```
   [
     {
       "Name": "web-function-invocations",
       "FieldSelectors": [
         {
   ```

```
        "Field": "eventCategory",
        "Equals": ["Data"]
      },
      {
        "Field": "resources.type",
        "Equals": ["AWS::Lambda::WebFunction"]
      },
      {
        "Field": "resources.ARN",
        "Equals": [
          "arn:aws:lambda:us-east-1:111122223333:web-function/my-web-app"
        ]
      }
    ]
  }
]
```

3. Appliquez le sélecteur à la piste :

```
aws cloudtrail put-event-selectors \
    --trail-name my-trail \
    --advanced-event-selectors file://web-function-data-events.json
```

> **Important**
>
> `put-event-selectors`remplace les sélecteurs d'événements existants du sentier. Si le parcours enregistre déjà d'autres événements, incluez leurs sélecteurs dans le même fichier.

4. Appelez le point de terminaison avec une demande de test.
5. Recherchez la destination du sentier pour`eventName = InvokeWebFunctionEndpoint`. Vérifiez l'ARN de la fonction, l'heure de l'événement, l'ID de la demande, les informations sur l'appelant disponibles pour le chemin d'authentification et les éventuels champs d'erreur conditionnelle. Si le sélecteur fonctionne, la requête renvoie un `InvokeWebFunctionEndpoint` événement pour votre demande de test, comme dans l'exemple présenté dansthe section called “Exemple : appel réussi (appelant non authentifié)”.

Pour enregistrer des événements de données dans un magasin de données d'événements CloudTrail Lake à la place, ajoutez les mêmes sélecteurs de champs au magasin de données d'événements. Pour plus d'informations, consultez le Guide de l'utilisateur AWS CloudTrail .

Champs d'un InvokeWebFunctionEndpoint événement

Le tableau suivant décrit les champs d'un `InvokeWebFunctionEndpoint` événement.

Champ	Remarques
`eventVersion`	Version du format de l'événement .
`eventSource`	Toujours `lambda.amazonaws.com` .
`eventName`	Toujours `InvokeWebFunctionEndpoint` .
`eventCategory`	Toujours `Data`.
`eventType`	Le type d'événement, par exemple`AwsApiCall` .
`readOnly`	Toujours`false`, car un appel exécute votre code de fonction.
`managementEvent`	Toujours `false`.
`eventTime`	Date et heure, en UTC, auxquelles Lambda a enregistr é l'événement. Pour un appel réussi, Lambda enregistre l'événement lorsque votre fonction commence sa réponse, `eventTime` ce qui peut être postérieur à l'heure d'arrivée de la demande.
`sourceIPAddress`	Adresse IP à partir de laquelle la demande a été faite.
`userAgent`	L'agent utilisé par l'appelant pour effectuer la demande. Présent lorsque l'appelant envoie un `User-Agent` en-tête.
`requestParameters`	Contient `endpointArn` l'ARN du point de terminaison invoqué. La charge utile de la demande n'est pas enregistrée.
`responseElements`	Toujours `null`.

Champ	Remarques
`resources`	Contient une entrée avec le `accountId` `type`, et `ARN` de la fonction.
`additionalEventData`	Contient `functionRevisionArn` l'ARN de la révision qui a répondu à la demande. Ce champ est présent sur tous les événements, y compris les refus.
`tlsDetails`	Version TLS, suite de chiffrement et en-tête hôte de la demande.
`userIdentity`	L'identité de l'appelant. Pour plus de détails, consultez la liste suivante.
`sharedEventID`	Présent lorsque CloudTrail le même événement est diffusé à plus d'une personne Compte AWS.
`errorCode` , `errorMessage`	Présent uniquement en cas d'erreur.
`requestID` , `eventID`, `recipientAccountId` , `awsRegion`	CloudTrail Champs standard qui identifient la demande, l'événement, le destinataire Compte AWS et le Région AWS.

Les événements Web Function utilisent les formes d'ARN suivantes :

- Fonction (`resources[].ARN`) — `arn:aws:lambda:us-east-1:123456789012:web-function/my-fn`
- Point de terminaison (`requestParameters.endpointArn`) — `arn:aws:lambda:us-east-1:123456789012:web-function/my-fn/endpoint/my-endpoint`
- Révision (`additionalEventData.functionRevisionArn`) — `arn:aws:lambda:us-east-1:123456789012:web-function/my-fn/revision/rev-a1b2c`

Le `userIdentity` champ dépend de la manière dont l'appelant s'est authentifié :

- Les invocations non authentifiées sont enregistrées avec le type. `userIdentity` `Unknown`

- IAM-authenticated les appelants sont enregistrés avec leur propre directeur. Par exemple, un appelant utilisant des informations d'identification temporaires apparaît avec les `AssumedRole` caractères type`arn`, an et a. `sessionContext`
- Le champ `accessKeyId` n'est pas renseigné.

Événements d’erreur

CloudTrail enregistre également les tentatives d'invocation qui échouent une fois que l'appelant est authentifié. Le tableau suivant décrit ces événements d'erreur.

Scénario	errorCode	errorMessage
Appelant non autorisé	`AccessDenied`	L'utilisateur n'est pas autorisé à effectuer : `lambda:InvokeWebFunctionEndpoint`
Taux de demande, simultanéité ou limite de vCPU atteinte (point de terminaison ou compte)	`ThrottlingException`	Vitesse de transfert dépassée
Défaut de service	`ServiceException`	Erreur de service
Erreur d'application ou demande client non valide	Non applicable	Considéré comme un appel d'API réussi. L'invocation a atteint et exécuté la fonction.

Une invocation réussie ne comporte aucun `errorCode` ou`errorMessage`. Les refus d'autorisation sont enregistrés sous `AccessDenied` le nom de. CloudTrail n'enregistre pas les demandes qui échouent à l'authentification, telles que les demandes dont la signature est manquante, mal formée, non valide ou expirée, et n'enregistre pas les demandes rejetées par Lambda avant l'authentification, telles que les demandes adressées à un point de terminaison `rateLimit` dont la valeur est 0. Les défaillances de l'infrastructure d'authentification interne ne sont pas non plus enregistrées. Pour détecter un pic de demandes rejetées, lancez une alarme `HTTPResponseStatusClass4XX` dans l'espace de `AWS/Lambda/Web` noms.

Exemple : appel réussi (appelant non authentifié)

L'exemple suivant montre un appel réussi par un appelant non authentifié.


```
{
    "Records": [
        {
            "eventVersion": "1.11",
            "userIdentity": {
                "type": "Unknown"
            },
            "eventTime": "2026-09-22T18:41:07Z",
            "eventSource": "lambda.amazonaws.com",
            "eventName": "InvokeWebFunctionEndpoint",
            "awsRegion": "us-east-1",
            "sourceIPAddress": "203.0.113.42",
            "userAgent": "curl/8.4.0",
            "requestParameters": {
                "endpointArn": "arn:aws:lambda:us-east-1:123456789012:web-function/my-
fn/endpoint/my-endpoint"
            },
            "responseElements": null,
            "additionalEventData": {
                "functionRevisionArn": "arn:aws:lambda:us-east-1:123456789012:web-
function/my-fn/revision/rev-a1b2c"
            },
            "requestID": "b1f8a4c2-7e3d-4a19-9f6b-2c5d8e0a1234",
            "eventID": "d4c3b2a1-5f6e-7a8b-9c0d-1e2f3a4b5c6d",
            "readOnly": false,
            "resources": [
                {
                    "accountId": "123456789012",
                    "type": "AWS::Lambda::WebFunction",
                    "ARN": "arn:aws:lambda:us-east-1:123456789012:web-function/my-fn"
                }
            ],
            "eventType": "AwsApiCall",
            "managementEvent": false,
            "recipientAccountId": "123456789012",
            "eventCategory": "Data",
            "tlsDetails": {
                "tlsVersion": "TLSv1.3",
                "cipherSuite": "TLS_AES_128_GCM_SHA256",
```

```
                "clientProvidedHostHeader": "bcdfghjklmnpqrst.b7t.lambda-web.us-
east-1.on.aws"
            }
        }
    ]
}
```

Pour un IAM-authenticated appelant, le `userIdentity` champ contient plutôt le principal de l'appelant, par exemple tapez `AssumedRole` avec un `arn` et un`sessionContext`, et les champs restants restent inchangés.

Exemple : invocation refusée

Les événements d'erreur comportent `errorCode` et`errorMessage`. L'exemple suivant montre un appel refusé.

```
{
    "Records": [
        {
            "eventVersion": "1.11",
            "userIdentity": {
                "type": "AssumedRole",
                "principalId": "ARO01EXAMPLEID:session-name",
                "arn": "arn:aws:sts::123456789012:assumed-role/app-invoke-role/session-
name",
                "accountId": "123456789012",
                "sessionContext": {
                    "sessionIssuer": {
                        "type": "Role",
                        "principalId": "ARO01EXAMPLEID",
                        "arn": "arn:aws:iam::123456789012:role/app-invoke-role",
                        "accountId": "123456789012",
                        "userName": "app-invoke-role"
                    },
                    "attributes": {
                        "creationDate": "2026-09-22T18:39:55Z",
                        "mfaAuthenticated": "false"
                    }
                }
            },
            "eventTime": "2026-09-22T18:42:13Z",
            "eventSource": "lambda.amazonaws.com",
            "eventName": "InvokeWebFunctionEndpoint",
```

```
            "awsRegion": "us-east-1",
            "sourceIPAddress": "203.0.113.42",
            "userAgent": "aws-sdk-python/1.34.0",
            "errorCode": "AccessDenied",
            "errorMessage": "User is not authorized to perform:
 lambda:InvokeWebFunctionEndpoint",
            "requestParameters": {
                "endpointArn": "arn:aws:lambda:us-east-1:123456789012:web-function/my-
fn/endpoint/my-endpoint"
            },
            "responseElements": null,
            "additionalEventData": {
                "functionRevisionArn": "arn:aws:lambda:us-east-1:123456789012:web-
function/my-fn/revision/rev-a1b2c"
            },
            "requestID": "c2e9b5d3-8f4e-4b2a-a07c-3d6e9f1b2345",
            "eventID": "e5d4c3b2-6a7f-8b9c-0d1e-2f3a4b5c6d7e",
            "readOnly": false,
            "resources": [
                {
                    "accountId": "123456789012",
                    "type": "AWS::Lambda::WebFunction",
                    "ARN": "arn:aws:lambda:us-east-1:123456789012:web-function/my-fn"
                }
            ],
            "eventType": "AwsApiCall",
            "managementEvent": false,
            "recipientAccountId": "123456789012",
            "eventCategory": "Data",
            "tlsDetails": {
                "tlsVersion": "TLSv1.3",
                "cipherSuite": "TLS_AES_128_GCM_SHA256",
                "clientProvidedHostHeader": "bcdfghjklmnpqrst.b7t.lambda-web.us-
east-1.on.aws"
            }
        }
    ]
}
```

Événements de gestion dans CloudTrail

CloudTrail enregistre les événements de gestion des fonctions Web par défaut. Vous pouvez consulter les événements de gestion des 90 derniers jours dans l' CloudTrail historique des

événements sans créer de trace. Pour les conserver plus longtemps, créez une banque de données sur les événements CloudTrail relatifs aux sentiers ou aux lacs. Pour plus d'informations, consultez Journalisation des événements de gestion dans le Guide de l'utilisateur AWS CloudTrail .

CloudTrail enregistre les opérations de fonction Web suivantes en tant qu'événements de gestion. Le `eventName` champ de chaque événement est identique au nom de l'opération.

Ressource ou tâche	Opérations
Fonctions Web	`CreateWebFunction` , `GetWebFunction` , `ListWebFunctions` , `DeleteWebFunction`
Révisions	`CreateWebFunctionRevision` , `GetWebFunctionRevision` , `ListWebFunctionRevisions` , `DeleteWebFunctionRevision`
Points de terminaison	`CreateWebFunctionEndpoint` , `GetWebFunctionEndpoint` , `ListWebFunctionEndpoints` , `UpdateWebFunctionEndpoint` , `DeleteWebFunctionEndpoint`
Paramètres du compte	`GetWebAccountSettings`
Politiques basées sur une ressource	`PutResourcePolicy` , `GetResourcePolicy` , `DeleteResourcePolicy`
Étiquettes	`TagResource` , `UntagResource` , `ListTags`

L'invocation d'une fonction Web est une opération de plan de données. CloudTrail l'enregistre uniquement en tant qu'événement de données, comme décrit dansthe section called "Événements de données de fonction Web dans CloudTrail".

Ressources connexes

Pour plus d'informations, consultez les ressources suivantes :

- the section called "CloudTrail journaux"
- the section called "Permissions"
- Création d'un parcours pour votre Compte AWS

Exemples d'applications Web Function

Chaque échantillon est utilisé `index.js` comme fichier d'entrée et écoute l'hôte et le port depuis`AWS_LAMBDA_HTTP_ENDPOINT`. Package l'application avec ses dépendances de production et déployez-la à partir d'un objet Amazon S3 versionné.

Le tableau suivant répertorie chaque exemple et les enseignements que vous pouvez en tirer.

Exemple	Utilisez-le pour apprendre
the section called “Minimale Express vigie”	Démarrez un serveur HTTP avecExpress.
the section called “Honneur API et fichiers statiques”	Servez des routes d'API et des fichiers statiques avecHono.
the section called “Server-sent événements”	Diffusez les événements envoyés par le serveur et arrêtez le travail lorsque le client se déconnecte.
the section called “Multi-Region itinéraire de vérification”	Renvoie la région de desserte lors de la validation du routage multirégional.

Minimale Express vigie

Cet exemple basé sur un framework est une alternative au démarreur sans dépendance créé par. `--hello-world` Pour le déploiement initial, voirthe section called “Déployez et testez votre fonction Web”.

Installez Express :

```
npm init -y
npm install express
```

Créez `index.js` :

```
const express = require('express');
const app = express();
const [host, port] = (process.env.AWS_LAMBDA_HTTP_ENDPOINT ||
 'localhost:3000').split(':');

app.get('/', (request, response) => {
  response.send('Hello from Lambda Web Functions!');
});

app.listen(port, host);
```

Pour des conseils d'emballage, voirthe section called “Package et déploiement d'un échantillon”.

Honneur API et fichiers statiques

Installez les dépendances :

```
npm init -y
npm pkg set type=module
npm install hono @hono/node-server
```

Créez `index.js` :

```
import { serve } from '@hono/node-server';
import { serveStatic } from '@hono/node-server/serve-static';
import { Hono } from 'hono';
import { secureHeaders } from 'hono/secure-headers';

const app = new Hono();
app.use(secureHeaders());
app.use('/static/*', serveStatic({ root: './' }));
app.get('/api/health', (context) => context.json({ status: 'ok' }));
app.notFound((context) => context.json({ error: 'not found' }, 404));

const [host, port] = (process.env.AWS_LAMBDA_HTTP_ENDPOINT ||
 'localhost:3000').split(':');

serve({ fetch: app.fetch, port: Number(port), hostname: host });
```

Placez les fichiers statiques dans un `static` répertoire et incluez le répertoire dans le package de déploiement.

Server-sent événements

Ajoutez l'itinéraire suivant à une Express application :

```
app.get('/events', (request, response) => {
  response.setHeader('Content-Type', 'text/event-stream');
  response.setHeader('Cache-Control', 'no-cache');
  response.flushHeaders();

  const interval = setInterval(() => {
    response.write(`data: ${JSON.stringify({ time: Date.now() })}\n\n`);
  }, 1000);

  response.on('close', () => {
    clearInterval(interval);
  });
});
```

La demande reste active jusqu'à ce que l'application mette fin à la réponse ou que le client se déconnecte. Définissez le délai de révision pour la durée maximale du stream. WebSocketles mises à niveau ne sont pas prises en charge.

Multi-Region itinéraire de vérification

Ajoutez une route qui renvoie la région dans laquelle la demande a été exécutée :

```
app.get('/region', (request, response) => {
  response.json({
    region: process.env.AWS_REGION,
    requestId: request.get('lambda-web-request-id')
  });
});
```

Appelez l'itinéraire depuis les sites clients concernés par votre application. Pour un `MultiRegion` point de terminaison, la région sélectionnée provient d'un routage basé sur la latence et peut changer. N'utilisez pas l'environnement d'exécution comme magasin de sessions.

Package et déploiement d'un échantillon

```
npm ci --omit=dev
```

```
zip -r function.zip index.js package.json package-lock.json node_modules
aws s3 cp function.zip s3://amzn-s3-demo-bucket/samples/function.zip
```

Incluez d'autres fichiers utilisés par l'échantillon sélectionné, tels que le `static` répertoire de l'Honoexemple. Pour créer une révision qui fait référence à l'objet chargé, reportez-vous the section called “Code dans Amazon S3” aux sections etthe section called “Révisions”. Pour le `deploy` flux de travail de niveau supérieur, voir. the section called “Création d'une fonction Web (AWS CLI)” Une fois que la révision est terminée `Active` et que le point de terminaison l'a traitée, envoyez une demande au domaine du point de terminaison pour confirmer les réponses de l'échantillon. Pour la couverture du test au-delà de ce test de fumée, voirthe section called “Tests”.

Bonnes pratiques pour les fonctions Web Lambda

Sécurisez tous les terminaux

Chaque point de terminaison est accessible depuis Internet. La manière dont vous authentifiez les appelants, installez une porte d'entrée et définissez les autorisations détermine qui peut accéder à votre application et à quoi elle peut accéder. Suivez les pratiques suivantes :

- Chaque point de terminaison est accessible depuis Internet, quel que soit son type d'authentification. Avec`ApplicationManaged`, Lambda n'authentifie pas les demandes, de sorte que tout client connaissant le domaine peut appeler votre application. Mettez en œuvre l'authentification, l'autorisation, la validation des entrées, le contrôle de la taille des demandes et la protection contre les abus dans l'application ou dans une porte d'entrée.
- `IamAuth`À utiliser lorsque les appelants peuvent signer des demandes et que les politiques IAM fournissent le modèle d'autorisation requis. Élargissez les politiques de ressources aux ARN et aux principaux spécifiques des terminaux.
- Placez Amazon CloudFront ou Amazon API Gateway devant un point de terminaison lorsque vous avez besoin d'un domaine personnalisé, d'une AWS WAF inspection, d'une mise en cache ou de contrôles périphériques centralisés. Limitez l'origine afin que les clients ne puissent pas contourner la porte d'entrée. Avec CloudFront, utilisez un contrôle d'accès aux points de `IamAuth` terminaison et aux origines (OAC), comme décrit dansthe section called “CloudFront intégration”. Avec les autres portes d'entrée, le point de terminaison reste directement accessible. Vérifiez donc un secret ou un jeton partagé dans l'application.
- Utilisez un rôle d'exécution dédié avec des autorisations de moindre privilège. Séparez l'identité de déploiement, le téléchargeur de code, le principal du service Lambda, le rôle d'exécution et les autorisations de l'appelant du point de terminaison.

- Ne mettez pas de secrets dans les packages ou les journaux de déploiement. Chargez les secrets au moment de l'exécution à partir d'un magasin de secrets approprié, mettez-les en cache uniquement le temps nécessaire et supprimez les champs de requête sensibles.

Conservez les artefacts de déploiement immuables

- Activez le versionnement dans le compartiment de code et enregistrez l'ID de version de l'objet pour chaque déploiement.
- Ne remplacez ni ne supprimez les versions d'objets utilisées par les révisions actives ou annulées. Conservez l'accès principal au service Lambda tant qu'une révision fait référence à l'objet.
- Créez des packages de déploiement dans un pipeline reproductible. Installez les dépendances de production à partir d'un fichier de verrouillage, excluez les fichiers de développement et testez l'archive exacte avant le téléchargement.
- Créez des dépendances natives pour Arm64. Un module natif créé pour x86_64 ne s'exécute pas dans l'environnement d'exécution des fonctions Web.
- Utilisez des compartiments, des préfixes, des rôles ou des comptes distincts lorsque les environnements ont des exigences de confiance ou de rétention différentes.

Conception pour les demandes simultanées

- Conservez les données spécifiques à la demande dans le champ d'application de la demande. Ne stockez pas les informations d'identification, les données client, les objets de réponse ou l'état modifiable par demande dans des variables globales.
- Utilisez le mode asynchrone I/O. Le fonctionnement synchrone du processeur ou du système de fichiers bloque la boucle d'Node.jsévénements et retarde chaque demande en cours dans l'environnement.
- `worker_threads`À utiliser pour les CPU-intensive travaux qui doivent utiliser plusieurs vCPU ou moins `maxConcurrencyPerEnvironment` afin de réduire les conflits.
- Tenez compte du Node.js tas séparément de la mémoire de l'environnement. L'environnement dispose de 2 Go, tandis que le segment de mémoire V8 par défaut est de 1 024 Mo. Si vous augmentez le tas avec `--max-old-space-size` in`NODE_OPTIONS`, laissez de la mémoire pour les tampons, les modules natifs, le runtime et les requêtes simultanées.

- Réutilisez les clients initialisés et les pools de connexions entre les demandes, mais validez les connexions périmées et la croissance du cache liée. Conserve l'état requis en dehors de l'environnement d'exécution.
- Maintenez les connexions sortantes actives afin que les demandes adressées aux bases de données et autres dépendances les réutilisent au lieu d'ouvrir une nouvelle connexion à chaque fois. Node.jsactive keep-alive par défaut dans son agent HTTP global. Si vous créez votre propre agent ou configurez un client SDK, maintenez Keep-Alive activé. Gérez également les connexions que la télécommande ferme lorsqu'elles sont inactives.
- Utilisez des noms uniques pour les fichiers temporaires et supprimez-les lorsqu'ils ne sont plus nécessaires. Plusieurs demandes partagent le système de fichiers de 512 Mo `/tmp` de l'environnement, et les fichiers peuvent être conservés d'une demande à l'autre jusqu'à ce que l'environnement soit supprimé.

Assurez la prévisibilité du démarrage

- Démarrez rapidement le serveur HTTP et écoutez la valeur exacte de`AWS_LAMBDA_HTTP_ENDPOINT`.
- Conservez la taille du package et supprimez les dépendances de production inutilisées.
- Initialisez uniquement les ressources nécessaires pour que le serveur puisse accepter le trafic. Effectuez des tâches facultatives avec paresse, mais évitez que les demandes simultanées ne dupliquent une initialisation coûteuse.
- Gérez `SIGTERM` le nettoyage qui se termine en 1 seconde, mais ne vous fiez pas aux rappels d'arrêt pour conserver les données requises.

Définissez des limites à partir du comportement mesuré

- Test de charge avec les mêmes dépendances applicatives et les mêmes services en aval que ceux utilisés en production. Augmentez la simultanéité jusqu'à ce que la latence, la consommation du processeur, la mémoire ou la capacité en aval deviennent la contrainte contraignante.
- `maxConcurrencyPerEnvironment`À utiliser pour limiter le contentieux par processus, `maxEnvironments` pour limiter l'échelle horizontale et `rateLimit` pour protéger les dépendances en aval contre les rafales de demandes.

- Vérifiez les limites de compte et régionales appliquées avant les tests de performances et les lancements. La configuration du point de terminaison ne peut pas créer de capacité au-delà d'une limite de compte.
- Réessayez les réponses HTTP 429 et les réponses HTTP 503 sans `lambda-web-error-type` en-tête. Utilisez le backoff et le jitter, et réessayez uniquement lorsque l'opération est idempotente. Utilisez des clés d'idempuissance ou une déduplication au niveau de l'application pour les écritures.

Déploiement avec vérification et annulation explicites

- Utilisez des pondérations de révision manuelles pour les points finaux de production. Maintenez le déploiement automatique des dernières révisions pour les environnements de développement dans lesquels un déploiement immédiat est acceptable.
- Attendez que la nouvelle révision soit disponible `Active` et que la mise à jour du terminal soit terminée avant de l'évaluer. Pour les `PerRegion` terminaux `MultiRegion` et les terminaux, vérifiez l'état de mise à jour dans chaque région.
- Utilisez des journaux d'applications ou des métriques personnalisées qui incluent l'identifiant de révision lors des déploiements Canary. Service-vended les métriques n'incluent pas de dimension de révision.
- Avant de transférer le trafic, définissez les indicateurs auxquels une nouvelle révision doit répondre et la durée pendant laquelle vous les observez (critères de stabilisation), ainsi que les seuils déclenchant une annulation. Conservez la version de l'objet de code, l'accès par clé et la configuration de la révision précédente jusqu'à la fin de la fenêtre de restauration. Lambda supprime automatiquement les révisions les plus anciennes vers lesquelles aucun point de terminaison n'est acheminé lorsqu'une fonction Web dépasse sa limite de révision. Conservez donc la révision d'annulation sur un point de terminaison (par exemple, un point de terminaison de test) ou soyez prêt à la recréer à partir de la même version d'objet. Pour plus de détails, consultez the section called “Limites de révision et nettoyage automatique”.

Établissez une base de référence opérationnelle

- Émettez des journaux d'applications structurés avec l'ID de demande, l'ID de révision, l'itinéraire, le code d'état, la durée et les identifiants nécessaires pour diagnostiquer les défaillances en aval. N'enregistrez pas les informations d'identification, les jetons ou les corps de demande sensibles.

- Alarmez en cas de réponse et de limitation 5xx, et surveillez les demandes exécutées, les environnements actifs et la capacité du compte. Configurez des mesures d'erreur éparses pour traiter les données manquantes de manière appropriée.
- Utilisez l'ID de demande de réponse et les en-têtes du flux de journal pour corréler les défaillances des clients avec les journaux. Activez les journaux système DEBUG uniquement lorsque vous avez besoin des événements supplémentaires.
- Enregistrez les opérations de gestion et les événements liés aux données d'invocation des terminaux AWS CloudTrail lorsque vos exigences d'audit en ont besoin.

Fonctionnement MultiRegion et PerRegion terminaux en tant que systèmes distribués

- Rendez les données d'application, les secrets, les clés et les dépendances en aval disponibles dans toutes les régions susceptibles de recevoir du trafic.
- Testez les échecs de déploiement partiels et les échecs de dépendance régionale. Ne partez pas du principe que toutes les régions exécutent la même révision tant que chaque mise à jour régionale n'indique un succès.
- Après chaque mise à jour du terminal, vérifiez `updateStatus` chaque entrée`regionalEndpoints`. La réplication peut échouer dans certaines régions alors qu'elle réussit dans d'autres. Par conséquent, une mise à jour peut être partiellement appliquée. Réessayez ou revenez en arrière avant de considérer le déploiement comme terminé.
- Pour les `PerRegion` terminaux, testez votre DNS externe ou votre basculement frontal indépendamment du déploiement de la fonction Web.
- Centralisez les vues opérationnelles dans la région d'origine, mais maintenez une trajectoire de reprise en cas de retard ou d'interruption de la télémétrie.

Test des fonctions Web Lambda

Les fonctions Web exécutent des serveurs HTTP standard, ce qui vous permet de tester le comportement de la plupart des applications localement à l'aide des outils habituels de votre infrastructure. Des tests dans le cloud sont toujours nécessaires pour valider l'autorisation IAM, l'accès à Amazon S3 et AWS Key Management Service (AWS KMS), les états du cycle de vie des fonctions Web, le dimensionnement, la télémétrie et le comportement multirégional.

Couches de test recommandées

Le tableau suivant décrit chaque couche de test, ce qu'elle valide et où elle s'exécute.

Couche de test	Ce qu'il valide	Où il fonctionne
Unit	Logique métier, validation, décisions d'autorisation, sérialisation et gestion des erreurs.	Développement local et environnements de construction.
intégration HTTP	Routes, intergiciels, en-têtes, streaming, délais d'attente, déconnexions gracieuses et comportement du framework.	Contre un serveur de production exécuté localement.
Package	Fichier d'entrée, dépendances de production, mise en page de l'archive, démarrage et utilisation par le serveur de`AWS_LAMBDA_HTTP_ENDPOINT` .	À partir de l'archive exacte que le pipeline de déploiement télécharge.
Intégration dans le cloud	IAM, politiques relatives aux compartiments, clés, états du cycle de vie, comportement des terminaux, télémétrie et appels de service en aval AWS .	Dans un environnement isolé Compte AWS ou de test.
Charge et résilience	Sécurité de la simultanéité, latence, régulation, limites en aval, annulation et comportement régional en cas de défaillance.	Dans un environnement cloud de type production avec des contrôles explicites des coûts et du trafic.

Exécutez le serveur HTTP localement

Utilisez une solution de remplacement locale pour`AWS_LAMBDA_HTTP_ENDPOINT`, comme indiqué dans lethe section called “Minimale Express vigie”. Vous pouvez également définir la variable de manière explicite pour tester le même chemin de démarrage utilisé par Lambda :

```
AWS_LAMBDA_HTTP_ENDPOINT=127.0.0.1:3000 node index.js
```

Envoyez des demandes avec votre client HTTP normal et vérifiez les codes d'état, les corps de réponse, les en-têtes, la validation des demandes, le middleware d'authentification, les délais d'expiration, le streaming et la gestion des déconnexions du client.

Exécutez des demandes simultanées lors des tests d'intégration locaux. Vérifiez l'état global de la demande, les caches mutables partagés, l'initialisation en double, les collisions de noms de fichiers et le blocage des boucles d'événements.

Testez le package de déploiement

1. Installez les dépendances à partir du fichier de verrouillage validé et créez l'archive à l'aide des mêmes commandes que le pipeline de déploiement.
2. Extrayez l'archive dans un répertoire propre. Exécutez l'application à partir de ce répertoire sans accéder aux dépendances de développement ni aux fichiers source non suivis.
3. Vérifiez que le fichier d'entrée configuré existe sur le chemin attendu et démarrez le serveur HTTP.
4. Enregistrez la somme de contrôle de l'archive et l'ID de version de l'objet Amazon S3 utilisés par la révision. Utilisez ces valeurs pour identifier l'artefact exact testé.

Les fonctions Web s'exécutent sur Arm64. Lorsqu'un package contient des dépendances natives, créez et testez ces dépendances pour Linux Arm64 plutôt que de réutiliser les artefacts d'un ordinateur de développement x86-64. Par exemple, vous pouvez installer des dépendances de production dans un conteneur Arm64 :

```
docker run --rm --platform linux/arm64 \
    --volume "$PWD":/app \
    --workdir /app \
    node:24 \
    npm ci --omit=dev
```

Testez dans un environnement cloud isolé

1. Téléchargez l'archive testée dans un compartiment Amazon S3 versionné et créez une révision qui fait référence à la version de l'objet obtenue.
2. Interrogez la révision jusqu'à ce qu'elle devienne `Active` ou`Failed`. Echouez le test avec le rapport `stateReason` au lieu d'attendre indéfiniment.

3. Créez ou mettez à jour un point de terminaison de test. Sondage à la fois `state` et`updateStatus`. Pour les `PerRegion` terminaux `MultiRegion` et les terminaux, vérifiez chaque statut régional.
4. Envoyez des demandes au point de terminaison et vérifiez la réponse de l'application`lambda-web-request-id`, les journaux, les métriques et les effets secondaires attendus en aval.
5. Supprimez le point de terminaison, la fonction, les objets de test, les groupes de journaux et les autres ressources de test une fois le test terminé.

Autorisation des tests et exposition

- En effet`IamAuth`, vérifiez que les demandes non signées échouent, que les principaux autorisés réussissent, que les principaux refusés échouent et que l'accès entre comptes nécessite à la fois des politiques d'identité et de ressources.
- Pour`ApplicationManaged`, testez les informations d'identification de l'application manquantes, expirées, mal formées ou insuffisantes. Testez l'autorisation séparément de l'authentification.
- Testez les demandes de pré-vol du navigateur, les origines autorisées et refusées, les demandes accréditées et les en-têtes de sécurité lorsque les navigateurs appellent le point de terminaison.
- Lorsqu'une porte d'entrée protège le terminal, vérifiez que les demandes d'origine directe sont refusées et que seuls l'identité de porte d'entrée ou le chemin réseau attendus peuvent l'invoquer.

Testez la simultanéité, la mise à l'échelle et la régulation

- Augmentez progressivement la charge tout en enregistrant la latence, les réponses 4xx et 5xx, les accélérateurs, les environnements actifs et l'utilisation en aval.
- Testez le configuré `rateLimit`et `maxEnvironments`, et `maxConcurrencyPerEnvironment` indépendamment. Utilisez l'en-tête de `lambda-web-error-type` réponse (`Platform.EndpointRequestThrottle`,`Platform.AccountRequestThrottle`,`Platform.Endpo` ou`Platform.EndpointConcurrentInitThrottle`) pour confirmer quelle limite a produit chaque réponse HTTP 429. Enregistrez séparément les réponses HTTP 503 qui n'ont pas `lambda-web-error-type` d'en-tête. Ces réponses peuvent indiquer un délestage temporaire ou une erreur interne. Pour plus de détails, consultez the section called “Types d'erreur liés aux fonctions Web”.
- Testez les pics de trafic et les démarrages à froid, et pas uniquement le débit en régime permanent.

- Utilisez des données de test uniques et des clés d'idempuissance. Ne réessayez pas automatiquement les requêtes non idempotentes lors d'un test de charge.
- Définissez des limites de trafic, de durée et de coût explicites avant de démarrer un test de charge. Coordonner les tests susceptibles d'affecter les quotas de comptes partagés ou les systèmes en aval.

Tester les déploiements et les annulations

Dans un environnement de test, déployez deux révisions et appliquez la même procédure de routage pondéré que celle utilisée en production. Vérifiez que vos journaux ou vos statistiques personnalisées peuvent attribuer des demandes à chaque révision. Déclenchez délibérément les conditions d'annulation, restaurez tout le trafic à la version précédente et confirmez que son objet de code et ses dépendances restent disponibles.

Pour un point de `PerRegion` terminaison `MultiRegion` ou un terminal, testez un échec partiel de mise à jour et vérifiez que l'automatisation de votre déploiement détecte l'échec du statut régional. Testez l'action de restauration et répétez la mise à jour du terminal après avoir corrigé la cause.

Résolution des problèmes liés aux fonctions Web Lambda

Commencez par l'état de la ressource, la réponse HTTP et les journaux de la demande. Les fonctions Web exposent un état distinct pour la fonction, la révision, le point de terminaison et chaque région d'un point de `PerRegion` terminaison `MultiRegion` ou d'un point de terminaison. La défaillance d'une ressource ne change pas toujours l'état des autres.

> **Note**
>
> Avant d'exécuter les commandes de diagnostic décrites dans cette rubrique, assurez-vous que vous disposez des droits d' AWS CLI accès et des autorisations nécessaires pour appeler les opérations de la fonction `get-*` Web Lambda.

Collecter des informations de diagnostic

1. Obtenez la fonction Web, la révision et le point de terminaison. Enregistrez chaque`state`, `stateReason`ou`updateStatus`, et chaque `updateStatusReason` valeur.

```
aws lambda-web get-web-function \
    --function-name my-web-app

aws lambda-web get-web-function-revision \
    --function-name my-web-app \
    --revision-id revision-id

aws lambda-web get-web-function-endpoint \
    --function-name my-web-app \
    --endpoint-name prod
```

*my-web-app*Remplacez-le par le nom de votre fonction, *revision-id* par la révision à inspecter et *prod* par le nom de votre point de terminaison.

2. Envoyez une demande et enregistrez le code d'état et les en-têtes de réponse.

```
curl --include https://endpoint-domain/path
```

L'`lambda-web-request-id`en-tête identifie la demande. Lorsqu'il est présent, l'`lambda-web-logstream`en-tête identifie le flux de journal Amazon CloudWatch Logs qui a traité la demande, et l'`lambda-web-error-type`en-tête identifie une erreur de plateforme.

3. Consultez les journaux des applications et du système dans le groupe de journaux centralisé de la région d'origine de la fonction Web. Pour les noms des groupes de logs et les conseils de corrélation, voirthe section called “Journaux”.
4. Pour les `PerRegion` terminaux `MultiRegion` et les terminaux, inspectez chaque entrée. `regionalEndpoints` Un état satisfaisant au niveau du point de terminaison ne signifie pas que la dernière mise à jour a réussi dans toutes les régions.

Problèmes de déploiement et de démarrage

Symptôme	Ce qu'il faut vérifier	Résolution
Une révision est `Failed`	La révision`stateReas on` , la version de l'objet Amazon S3 référencé , la politique du bucket, le rôle d'exécution, le	Corrigez la configuration sous-jace nte et créez une nouvelle révision. Les révisions sont immuables et une révision échouée ne revient pas à`Active`.

Symptôme	Ce qu'il faut vérifier	Résolution
	runtime et AWS KMS la clé.	
Le point de terminaison l'est`Active`, mais les demandes échouent lors du démarrage de l'application	Journaux du système et des applications pour détecter les erreurs de fichier d'entrée, les erreurs de dépendance ou un serveur qui n'écoute jamais. `AWS_LAMBDA_HTTP_ENDPOINT`	Exécutez l'application packagée localement, vérifiez le fichier d'entrée et les dépendances de production, et écoutez l'hôte et le port exacts fournis par Lambda. Déployez la correction en tant que nouvelle révision.
La mise à jour d'un terminal échoue	`updateStatusReason` sur le point de terminaison et, pour `MultiRegion` et pour les `PerRegion` points de terminaison, sur chaque entrée régionale.	Corrigez la dépendance signalée ou la défaillance régionale, puis appelez à `UpdateWebFunctionEndpoint` nouveau pour réessayer la mise à jour.
`does not have s3:GetObject sur create-web-function-revision`	Le code est lu depuis Amazon S3, et la politique du compartiment ou la politique d'identité de l'appelant ne disposent pas d'un accès en lecture.	Grant `s3:GetObject` et `s3:GetObjectVersion` à la fois dans la politique de compartiment (pour le service Lambda) et dans la politique d'identité de l'appelant.
`AccessDenied sur get-web-function-endpoint`	La politique IAM n'inclut `Resource` pas le point de terminaison.	Inclure `web-function/` *`name`*`/*` dans la politique`Resource`.

Pour éviter les échecs de déploiement répétés, validez la configuration et le démarrage dans une révision de test avant de créer une révision de production.

Erreurs de CLI et de package

Erreur ou symptôme	Cause	Résolution
`invalid choice: lambda-web`	La version installée est AWS CLI antérieure aux commandes Web Function.	Mettez à jour AWS CLI et vérifiez que aws lambda-web help les opérations de la fonction Web sont répertoriées.
`Unknown parameter: BuildConfig`	La demande utilise les noms des PascalCase membres.	Utilisez les membres de demande CamelCase présentés dans ce guide, `buildConfig` tels que`codeConfig`, et. `serviceConfig`
`Cannot find module '/var/task/index.js'`	Le fichier d'entrée requis est absent de la racine de l'archive.	`index.js`À placer à la racine du package de déploiement. Incluez tous les fichiers et dépendances de production qu'il importe.
`ERR_MODULE_NOT_FOUND` pour un dossier de candidature	L'archive omet un fichier source ou compilé importé par`index.js`.	Inspectez l'archive avecunzip -l, ajoutez le fichier manquant et créez une nouvelle révision.
`Application.TimeoutListenError`, ou HTTP 502 sur la première requête	L'application écoute uniquement sur une adresse de boucle, telle que `127.0.0.1` ou`localhost`, ou sur un port autre que celui d'entrée. `AWS_LAMBDA_HTTP_ENDPOINT`	Analysez `AWS_LAMBDA_HTTP_ENDPOINT` et écoutez exactement sur cet hôte et ce port.
`EMFILE` ou `too many open files`	L'application fuit des sockets, des fichiers ou des connexions à des bases de données lors de demandes simultanées.	Fermez les descripteurs par demande, les pools de connexions liés et surveillez les descripteurs ouverts dans le cadre d'une simultanéité prolongée.

Erreur ou symptôme	Cause	Résolution
`JavaScript heap out of memory`	L'application a atteint la limite de mémoire V8 par défaut, qui est inférieure à la limite de mémoire de 2 Go de l'environnement d'exécution, ou les demandes simultanées ont épuisé la mémoire restante de l'environnement.	Vérifiez les objets conservés et les caches illimités, et réduisez la simultanéité. Si l'application nécessite un tas plus important, définissez une limite de tas V8 plus importante avec in. `--max-old-space-size` `NODE_OPTIONS` Laissez de la mémoire pour les tampons, les allocations natives et le temps d'exécution.
`Cannot find moduleDépendance/ERR_MODULE_NOT_FOUND` au moment de l'exécution	`node_modules` n'était pas inclus dans le package de déploiement.	Installez les dépendances de production et incluez-les dans le package : exécutez`npm ci --omit=dev` , puis confirmez avec`unzip -l function.zip` .
Les fichiers statiques renvoient HTTP 404	L'application résout les chemins de fichiers relatifs au répertoire de travail ou les fichiers n'ont pas été empaquetés.	Résolvez les chemins depuis le répertoire du module (`__dirname` dans CommonJS ou `import.meta.dirname` dans les modules ES) et vérifiez que les fichiers se trouvent dans le package avec`unzip -l`.
Erreurs d'importation ESM, telles que « Impossible d'utiliser l'instruction d'importation en dehors d'un module »	`package.json` ne déclare pas le type de module.	Ajoutez `"type": "module"` ou utilisez CommonJS de manière cohérente. `package.json`

Défaillances des requêtes HTTP

Réponse	Cause courante	Résolution
HTTP 400	Le client a utilisé une méthode HTTP non prise en charge ou a envoyé une demande que le terminal n'a pas pu traiter.	Utilisez une méthode prise en charge et passez en revue les en-têtes et les limites des demandes dansthe section called “Comportement HTTP”.
HTTP 403	L'autorisation d'une `IamAuth` demande a échoué pour l'une des raisons suivantes : • La demande n'est pas signée. • La demande omet l'en-tête de hachage de contenu requis. • La signature de la demande n'est pas valide. • L'appelant n'a pas l'autorisation. Pour les appels entre comptes, la politique d'identité ou la politique basée sur les ressources peuvent être absentes.	Vérifiez que la demande inclut l'`X-Amz-Content-SHA256` en-tête requis, vérifiez la signature et vérifiez `lambda:InvokeWebFunctionEndpoint` les politiques d'identité et de ressources requises. Pour les exigences de signature, voirthe section called “Signature des requêtes”. Pour les exigences en matière d'autorisation, voirthe section called “Octroi d'une autorisation d'appel à un directeur”.
HTTP 404	L'application ne définit pas l'itinéraire demandé ou le client utilise un domaine de point de terminaison obsolète. L'`Host`en-tête peut également ne pas correspondre au domaine du point de terminaison. Si vous configurez une porte d'entrée telle qu'Amazon CloudFront pour transfére	Vérifiez le chemin actuel`domainName` , le chemin de la demande et les itinéraires de l'application. Utilisation `lambda-web-error-type` et journaux pour distinguer une réponse de plateforme d'une réponse d'application.

Réponse	Cause courante	Résolution
	r l'`Host`en-tête du visiteur vers l'origine, Lambda renvoie cette erreur avec `lambda-web-error-type` set to. `Platform.InvalidEndpoint`	
HTTP 409	Le point de terminaison ne l'est pas`Active`, ou le point de terminaison a été résolu selon une révision qui ne l'est pas`Active`.	Inspectez la révision et l'état des terminaux. Si c'est le cas`Pending`, attendez et réessayez ; si c'est le cas`Failed`, créez un nouveau point de terminaison. Pour les révisions, supprimez les révisions échouées ou inactives des pondérations des points de terminaison et créez une révision de remplacement si nécessaire.
HTTP 429	L'une des erreurs suivantes s'est produite : • La demande a dépassé une limite de débit pour les terminaux. • Le terminal a épuisé la capacité de l'environnement. • Le compte a atteint une limite de requêtes régionales ou de vCPU. • Trop d'environnements d'exécution s'initialisaient en même temps pour le point de terminaison.	Lisez l'`lambda-web-error-type` en-tête pour identifier la limite appliquée. Consultez the section called “Types d'erreur liés aux fonctions Web”. Passez en revue les mesures d'accélération (`EndpointRequestThrottles` ,`AccountRequestThrottles` , et`AccountActiveVCPUArm64Throttles`)`EndpointActiveEnvironmentThrottles` , les mesures de capacité active, les paramètres des terminaux et les limites de compte appliquées. L'initialisation simultanée throttling (`Platform.EndpointConcurrentInitThrottle`) n'incrémente pas une métrique d'accélération. Réessayez uniquement les requêtes idempotentes, en utilisant backoff et jitter.

Réponse	Cause courante	Résolution
HTTP 502	Votre application a échoué avant de commencer à envoyer des requêtes, Lambda n'a pas pu préparer l'environnement d'exécution de votre fonction Web ou votre application a renvoyé une réponse non valide.	Journaux d'utilisation `lambda-web-error-type` et du système pour identifier la cause. Consultez the section called “Types d'erreur liés aux fonctions Web”.
HTTP 503	L'application s'est bloquée lors du traitement d'une demande, le point de terminaison est désactivé ou Lambda n'a pas pu obtenir de capacité ou accéder à l'application.	Utilisez`lambda-web-error-type` , le cas échéant, les journaux des applications et du système pour identifier la cause. Consultez the section called “Types d'erreur liés aux fonctions Web”. Un 503 dépourvu `lambda-web-error-type` peut indiquer un délestage temporaire ou une erreur interne. Dans les deux cas, réessayez les requêtes idempotentes avec backoff et jitter.
HTTP 504	L'application n'a pas répondu dans le délai de révision (`Runtime.RequestTimeout`).	Vérifiez la révision `timeoutSeconds` et la latence en aval.
Autre HTTP 5xx	L'application a renvoyé un statut 5xx, ou Lambda a rencontré une erreur interne (`lambda-web-error-type` aucun en-tête).	Utilisez l'ID de demande, l'en-tête du flux de données, les journaux de l'application et les journaux du système pour identifier la source et vérifier l'état du processus.

Réponse	Cause courante	Résolution
La demande se bloque ou expire en raison d'un télécharg ement important ; les journaux indiquent que 0 octet n'a été reçu	Le gestionnaire a commencé à écrire la réponse alors que le corps de la demande était encore en train d'arriver. Le chemin de requête de la fonction Web est semi-dupl ex : Lambda transmet le corps complet de la requête avant de fournir la réponse de votre application.	Lisez le corps de la demande dans son intégrali té avant de rédiger la réponse. Les boîtiers d'une taille inférieure à environ 1 Mo s'adaptent aux sockets buffers et peuvent masquer cela.

Limites des en-têtes de demande

Deux limites s'appliquent aux en-têtes de demande. Lambda limite le bloc d'en-tête à 128 KiB et rejette les demandes plus importantes avant qu'elles n'atteignent votre fonction. Le serveur Node.js HTTP de votre fonction limite également le nombre de lignes d'en-tête qu'il accepte. Les deux renvoient des champs d'en-tête de demande HTTP 431 trop grands, comme indiqué dans le tableau suivant. Pour les limites de la plateforme, voirthe section called “Limites d'en-têtes”.

Symptôme	Cause	Résolution
HTTP 431 avec`lambda-web-error-type: Platform.HeaderToo Large` . Aucune invocation et aucune entrée dans le journal des applications.	La tête de demande dépasse 131 072 octets (128 KiB), mesurée sur la tête de demande complète lorsque le client l'envoie.	Réduisez la taille des en-têtes de demande. Cette limite ne peut pas être augmentée.
HTTP 431 avec `lambda-web-request-id` et `lambda-web-logstre am` mais non`lambda-web-`	La demande comporte plus de 1 000 lignes d'en-tête reçues par le Node.js serveur, y compris les en-têtes ajoutés par Lambda.	Augmentez `server.ma xHeadersCount` le code de votre serveur ou réduisez le nombre de lignes d'en-tête envoyées par le client.

Symptôme	Cause	Résolution
`error-type` . Le gestionnaire ne s'exécute pas.		

La limite de taille compte chaque octet de la tête de requête lorsque le client l'envoie. Cela inclut la ligne de requête, chaque ligne d'en-tête (y compris `Host` les en-têtes ajoutés par la bibliothèque cliente) et les terminateurs de ligne. Les en-têtes ajoutés par Lambda ne sont pas pris en compte dans la limite de taille.

Lorsqu'une demande dépasse la limite de taille, Lambda la rejette avant qu'elle n'atteigne votre fonction. La demande ne produit donc aucun appel ni entrée dans le journal de l'application. L'en-tête de `lambda-web-error-type` réponse identifie la cause.

La limite de Node.js nombre compte les lignes d'en-tête, et non les noms d'en-tête distincts. Un en-tête répété trois fois compte trois fois. Par conséquent, une demande qui accumule `x-forwarded-for` ou suit des en-têtes par le biais d'une chaîne de proxys peut atteindre la limite. Aucun en-tête ne doit paraître inhabituel pour que cela se produise. La limite est mesurée en fonction de la demande que reçoit votre fonction, qui inclut les en-têtes ajoutés par Lambda. Par conséquent, un client qui envoie un peu moins de 1 000 lignes d'en-tête peut l'atteindre. Lorsque cela se produit, la demande atteint votre environnement d'exécution et le Node.js serveur la rejette lors de l'analyse. Votre gestionnaire ne fonctionne pas. La réponse contient les `lambda-web-logstream` en-têtes `lambda-web-request-id` et, mais pas l'`lambda-web-error-type`en-tête.

Si votre application doit accepter un nombre de lignes d'en-tête supérieur à celui Node.js autorisé par défaut, augmentez la Node.js limite dans le code de votre serveur. Définissez `server.maxHeadersCount` le nombre de lignes d'en-tête à accepter ou définissez-le `0` pour désactiver le contrôle du Node.js comptage. La limite de taille de 128 KiB s'applique toujours.

```
const server = http.createServer(handler);
server.maxHeadersCount = 2000;
server.listen(port, host);
```

Il n'est pas nécessaire de modifier la limite de taille de l'Node.jsen-tête. Les environnements d'Node.jsexécution gérés le définissent pour qu'il corresponde à la limite de plate-forme, de sorte que la limite de plate-forme s'applique à la taille de l'en-tête. Vous ne pouvez pas augmenter la limite de plate-forme à partir du code de l'application.

Pour respecter les limites, déplacez l'état en bloc hors des en-têtes vers le corps de la demande, supprimez les cookies et réduisez les en-têtes de proxy et de suivi redondants avant que la demande n'atteigne le point de terminaison. Si une CloudFront distribution se trouve devant le point de terminaison, transmettez uniquement les en-têtes dont votre application a besoin dans la politique de demande d'origine.

Types d'erreur liés aux fonctions Web

Lorsqu'une demande adressée à un point de terminaison Web Function échoue, Lambda renvoie un en-tête de `lambda-web-error-type` réponse qui identifie le problème. La valeur utilise le format `<Prefix>.<ErrorReason>` : le préfixe indique où l'erreur s'est produite, et la raison indique la cause.

Préfixe	Où l'erreur s'est produite
`Platform.`	La couche de plateforme de Lambda, qui achemine et valide les demandes, vérifie les autorisations et applique les limites.
`Runtime.`	Le runtime géré qui charge et exécute votre fonction.
`Application.`	Votre code de fonction.

Par exemple, `Runtime.RequestTimeout` cela signifie que le runtime géré a signalé que votre fonction n'a pas répondu dans le délai d'expiration configuré et `Application.InitCodeError` que votre propre code d'initialisation a généré une erreur.

Lambda inclut l'`lambda-web-error-type`en-tête lorsque l'erreur a été provoquée par la demande elle-même ou par votre fonction, sa configuration ou son code. Lambda omet l'en-tête pour les erreurs de service internes et pour les échecs d'autorisation, de sorte qu'aucun détail n'est révélé à un appelant non autorisé. Une valeur indique un problème sur le chemin entre la plateforme Lambda et votre fonction. Sur le chemin de la demande, l'erreur identifie l'endroit où la demande a échoué. Sur le chemin de réponse, utilisez la valeur associée à la télémétrie de votre application pour comprendre ce qui s'est passé.

Error type (Type d'erreur)	Description
`Platform.MalformedRequest`	Lambda n'a pas pu analyser la demande, ou la ligne ou la méthode de demande n'ont pas été acceptées.
`Platform.MissingHostHeader`	La demande n'incluait pas d'en-tête Host, Lambda n'a donc pas pu résoudre le point de terminaison cible.
`Platform.InvalidEndpoint`	L'en-tête Host n'a pas été résolu vers un point de terminaison existant valide.
`Platform.HeaderTooLarge`	La section d'en-tête de la demande a dépassé la limite de taille d'en-tête Lambda.
`Platform.DisallowedHeader`	La demande contenait un en-tête que Lambda n'accepte pas. Lambda renvoie HTTP 400.
`Platform.UnsupportedHttpVersion`	La requête utilisait une version HTTP autre que celle HTTP/1.1 requise par les fonctions Web.
`Platform.CannotAssumeRole`	Lambda n'a pas pu assumer le rôle d'exécution de votre fonction.
`Platform.KMSDecryptionError`	Lambda n'a pas pu utiliser la AWS KMS clé configurée pour déchiffrer vos variables d'environnement ou les autres données requises pour initialiser votre fonction.
`Platform.InvalidNetworkConfiguration`	Une ressource réseau VPC dont dépend votre fonction n'est pas valide. Pour en trouver la cause, voirthe section called “Problèmes de réseau et de connectivité”.
`Platform.RevisionNotActive`	La révision de fonction ciblée par la demande n'est pas à l'état Actif. La révision est peut-être toujours en cours d'activation ou n'a pas pu être activée. Vérifiez l'état de la révision ; si l'activation est toujours en cours, réessayez après un court laps de temps.
`Platform.EndpointNotActive`	Le point de terminaison n'est pas dans l'état Actif. Le point de terminaison est peut-être toujours en cours de provisionnement

Error type (Type d'erreur)	Description
	ou peut être indisponible pour une autre raison. Vérifiez l'état du terminal ; s'il est toujours en cours de création, réessayez après un court laps de temps.
`Platform.EndpointDisabled`	Le point de terminaison `rateLimit` étant 0, Lambda rejette toutes les demandes via HTTP 503. Définissez `rateLimit` une valeur différente de zéro pour reprendre le trafic.
`Platform.AccountDisabled`	Les invocations de fonctions Web sont désactivées pour le compte. Lambda renvoie HTTP 403. Contacte AWS Support.
`Platform.AccountRequestThrottle`	Le quota de taux de demandes au niveau du compte a été dépassé.
`Platform.EndpointRequestThrottle`	Le quota de taux de demandes du point de terminaison a été dépassé.
`Platform.AccountActiveVCPUArm64Throttle`	Le quota de vCPU actif du compte a été atteint.
`Platform.EndpointMaxEnvThrottle`	La limite maximale d'environnements du point de terminaison a été atteinte.
`Platform.EndpointConcurrentInitThrottle`	Trop d'environnements d'exécution s'initialisaient en même temps pour le point de terminaison. Réessayez avec un recul exponentiel.
`Runtime.RequestTimeout`	Votre fonction n'a pas renvoyé de réponse dans le délai d'expiration configuré.
`Runtime.OutOfMemory`	Votre fonction a dépassé sa limite de mémoire et le processus a été arrêté.
`Runtime.Unreachable`	Le processus d'exécution s'est écrasé, a quitté ou a refusé la connexion.
`Runtime.Exit`	Le processus d'exécution s'est terminé entre les demandes.

Error type (Type d'erreur)	Description
`Runtime.ExitError`	Le processus d'exécution s'est terminé avec une erreur.
`Runtime.InvalidResponse`	Les en-têtes de réponse du moteur d'exécution dépassaient la mémoire tampon de lecture.
`Runtime.OriginRequestError`	Le processus de candidature a échoué lors du traitement d'une demande. Consultez les journaux des applications pour plus de détails.
`Runtime.ImportCodeError`	Le moteur d'exécution n'a pas pu importer ou résoudre votre point d'entrée, par exemple un module manquant ou un chemin incorrect.
`Runtime.InitTimeout`	Votre fonction a dépassé le délai d'initialisation lors du provisionnement du sandbox.
`Application.InitCodeError`	Votre code d'initialisation a généré une erreur avant que la fonction ne commence à traiter les demandes.
`Application.TimeoutListenError`	Votre code d'initialisation n'a pas commencé à écouter sur le port avant la date limite d'initialisation.

Pour les mesures de régulation qui identifient la limite appliquée (pour les typesPlatform.AccountRequestThrottle, Platform.EndpointRequestThrottlePlatform.AccountActiveVCPUArm64Throttle, et Platform.EndpointMaxEnvThrottle d'erreur), voir. the section called “Indicateurs régionaux d'utilisation et de limitation”

Des journaux ou des statistiques sont manquants

- Vérifiez que le rôle d'exécution peut créer des groupes de journaux et des flux et enregistrer les événements de journal à la fois pour le groupe de journaux de destination et pour son `.local` compagnon.
- Recherchez dans le groupe de journaux centralisé de la région d'origine. Ne créez pas de diagnostics qui dépendent d'une région de réplication ou de groupes de `.local` journaux temporaires.

- Réglez `systemLogLevel` le `DEBUG` moment où vous en avez besoin`platform.requestComplete`.
- Prévoyez un délai de transmission de la télémétrie après la création ou la mise à jour des ressources. Ne considérez pas l'absence temporaire d'une métrique ou d'un événement de journal comme la preuve qu'une demande n'a pas été exécutée.
- N'oubliez pas que les indicateurs sont rares. Configurez les alarmes pour traiter les mesures d'erreur manquantes comme ne constituant pas une violation, le cas échéant.

Si aucun journal d'application n'apparaît, il est possible que le rôle d'exécution ne dispose pas CloudWatch des autorisations Amazon Logs. Attachez la politique `AWSLambdaBasicExecutionRole` gérée au rôle d'exécution, ou accordez `logs:CreateLogGrouplogs:CreateLogStream`, et`logs:PutLogEvents`. Pour les autorisations requises, consultez the section called “Rôle d'exécution”.

Problèmes de stockage et de chiffrement du code

Version d'objet Amazon S3 manquante ou inaccessible

Vérifiez que le contrôle de version du bucket est toujours activé, que la version exacte de l'objet existe et que l'appelant et le principal du service Lambda disposent des autorisations de lecture requises. Si une révision active perd l'accès à la version de l'objet épinglé, créez une nouvelle révision qui fait référence à une version disponible. Pour plus de détails, consultez the section called “Code dans Amazon S3”.

AWS KMS échec d'accès

Vérifiez les autorisations de l'appelant, la politique en matière de clés, le contexte de chiffrement, l'état de la clé et l'autorisation du principal `kms:Decrypt` du service Lambda. Pour les points de `PerRegion` terminaison `MultiRegion` et les points de terminaison, vérifiez qu'une réplique de la AWS KMS clé multirégionale existe et qu'elle est utilisable dans chaque région cible. Pour plus de détails, consultez the section called “Chiffrement au repos”.

Problèmes liés **`MultiRegion`**aux **`PerRegion`**terminaux

Utilisez le `regionalEndpoints` champ pour identifier la région affectée. Comparez ses régions `stateReason` et `updateStatusReason` celles des régions saines. Vérifiez les quotas régionaux, les répliques AWS KMS clés, la disponibilité de l'environnement d'exécution et l'état de réplication

de la révision. Après avoir corrigé la cause, répétez la mise à jour du terminal. Pour le modèle de réplication, voirthe section called “Multi-Region déploiement”.

Pour un `MultiRegion` point de terminaison, le routage basé sur la latence (qui dirige les demandes vers la région présentant la latence mesurée la plus faible) ne garantit pas que chaque demande soit dirigée vers la région à latence la plus faible. Effectuez un test à partir de l'emplacement du client concerné et inspectez les journaux de l'application pour déterminer quelle région a traité la demande. Pour un `PerRegion` point de terminaison, vérifiez également la configuration de votre DNS externe ou de votre routage frontal.

Problèmes de réseau et de connectivité

La plupart des problèmes de connectivité proviennent d'une révision de service qui ne contient aucune référence de connecteur ou qui fait référence à une ancienne version de connecteur, ou de sous-réseaux de connecteurs, de groupes de sécurité ou d'itinéraires qui bloquent le trafic.

Utilisez la séquence suivante pour isoler un problème de connectivité :

1. Exécutez `get-web-function-endpoint`. Vérifiez le mode de déploiement automatique et confirmez quelles révisions reçoivent du trafic.
2. Exécuter `get-web-function-revision` pour chaque révision de service. Vérifiez que son état est correct `Active` et qu'il fait référence à la version de connecteur attendue.
3. Exécutez `aws lambda-core get-network-connector --identifier` avec l'ARN du connecteur indiqué dans la version`egressNetworkConnectorArn`. Confirmez que `State` c'est le cas `ACTIVE` et, si le connecteur a été mis à jour, c'`LastUpdateStatus`est le cas`Successful`. Sinon, utilisez `StateReasonCode` ou `LastUpdateStatusReasonCode` pour identifier la cause, telle que `InsufficientRolePermissions`ou`InvalidSubnet`, ou`SubnetOutOfIPAddresses`.
4. Testez la destination par adresse IP pour séparer l'accessibilité du réseau de la résolution DNS.
5. Vérifiez les itinéraires du sous-réseau du connecteur, les groupes de sécurité de destination et les ACL du réseau.
6. Consultez les journaux de flux VPC sur les sous-réseaux du connecteur.

Les symptômes courants sont les suivants.

Symptôme	Check
Internet public fonctionne, mais pas les ressources VPC	La version de service ne contient aucune référence de connecteur.
L'accès au VPC fonctionne pour certaines demandes	Le point de terminaison est acheminé vers deux révisions avec des configurations de connecteur différentes.
Une mise à jour du connecteur n'a aucun effet	La version de service fait référence à une ancienne version du connecteur.
L'accès public s'arrête après l'ajout d'un connecteur	Les sous-réseaux du connecteur ne disposent pas de la route NAT ou IPv6 requise.
Le délai d'expiration d'une destination VPC	Le groupe de sécurité de destination, la table de routage ou l'ACL réseau bloquent la connexion.
Les journaux de flux ne contiennent aucun enregistrement correspondant	Le trafic n'est pas entré dans le VPC. Vérifiez à nouveau la révision du service et la référence du connecteur.
Les noms privés échouent mais les connexions IP directes fonctionnent	Vérifiez les attributs DNS du VPC et les associations de zones hébergées privées.
IPv4 fonctionne mais IPv6 échoue	Vérifiez la version `DualStack` du connecteur, les routes IPv6 et les règles de sécurité IPv6.
La version de service est la même`Active`, mais la fonction ne peut pas atteindre les ressources VPC privées	La version de service ne définit pas de connecteur réseau de sortie (`egressNetworkConnectorArn`). Lisez le champ avec `get-web-function-revision` ; s'il est vide, créez une révision qui définit`egressNetworkConnectorArn`. Pour plus de détails, consultez the section called “Mise en réseau”.

Il n'existe aucun accès interactif à un environnement d'exécution de fonctions Web. Utilisez les journaux des applications, les en-têtes de réponse des points de terminaison, les champs d'état des ressources, CloudWatch les métriques et les journaux de flux VPC pour diagnostiquer les défaillances.

Préparer un bundle d'escalade

Si les vérifications précédentes ne permettent pas d'identifier la cause, collectez les informations suivantes avant d'ouvrir un AWS Support dossier. Cela permet à l'ingénieur de support de corréler le fonctionnement du plan de contrôle, le déploiement régional, les demandes et la télémétrie :

- L' Compte AWS ID, la région d'origine, le nom de la fonction, l'ID de révision, le nom du point de terminaison, le type de point de terminaison et les régions cibles.
- L'horodatage UTC et le chemin de demande pour les échecs représentatifs, ainsi que les en-têtes de `lambda-web-error-type` réponse HTTP et de statut. `lambda-web-request-id` `lambda-web-logstream`
- La fonction, la révision, le point de terminaison et les `updateStatusReason` valeurs régionales `state` `stateReason``updateStatus`,, et.
- Les événements pertinents du journal centralisé des applications et du système, les indicateurs de vitesse et de capacité, ainsi que le taux de trafic approximatif au moment où le problème s'est produit.
- La AWS CLI version et une copie expurgée de la demande de gestion. Supprimez les informations d'identification, les secrets d'application, les jetons et les données de demande sensibles.

Informations connexes

- the section called “Mise en réseau”
- the section called “Contrôle”

AWS Lambda MicroVM

Si vous créez une application dans laquelle plusieurs utilisateurs ou agents d'IA se connectent à un environnement informatique et exécutent du code (par exemple, des environnements de développement interactifs, des CI/CD systèmes ou des bacs à sable pour l'IA), vous avez besoin d'environnements de calcul qui démarrent rapidement, restent isolés entre les locataires et ne vous obligent pas à gérer des serveurs ou des réseaux.

AWS Lambda Les micromachines virtuelles sont spécialement conçues pour ces cas d'utilisation. Il s'agit d'environnements informatiques sans serveur qui fournissent une VM-level isolation grâce à des fonctionnalités complètes du système d'exploitation (par exemple, installation de packages système ou montage de systèmes de fichiers), à des vitesses de démarrage rapides basées sur des instantanés et à un contrôle précis du réseau d'entrée (accès aux ports, prise en charge de, gRPC) et du réseau de sortie (accès Internet public et accès VPC WebSockets). HTTP/2

Pour les cas d'utilisation interactifs tels que les environnements de développement interactifs et les sandbox d'IA, les environnements peuvent connaître de longues périodes d'inactivité lorsque les utilisateurs finaux passent à d'autres tâches ou lorsqu'ils attendent l'IA. Les micromachines virtuelles peuvent être suspendues lorsqu'elles sont inactives, préservant ainsi la mémoire et l'état du disque tout en réduisant les coûts. Lorsque le trafic arrive, ils reprennent. Vous pouvez activer la suspension et la reprise automatique ou programmatique pour réduire les coûts d'inactivité, tout en maintenant une disponibilité quasi instantanée lorsque vos utilisateurs finaux reviennent.

AWS Lambda Les microVM fournissent ces fonctionnalités de base grâce à la virtualisation Firecracker, qui alimente plus de 15 billions d'appels mensuels de Lambda Functions.

Consultez Créez votre première microVM pour démarrer. Pour de plus amples informations sur la tarification, veuillez consulter AWS Lambda Pricing (français non garanti). Pour en savoir plus sur la sécurité et les autorisations, consultezthe section called “Sécurité”. Pour en savoir plus sur l'observabilité, voirthe section called “Contrôle”. Pour obtenir des conseils opérationnels, voirthe section called “Bonnes pratiques”.

Comment fonctionnent les micromachines virtuelles Lambda

1. Vous regroupez le code de votre application et a `Dockerfile` dans une archive zip et vous le chargez sur Amazon S3.

2. Vous appelez l'API Lambda pour créer une image microVM. Lambda exécute votre application`Dockerfile`, démarre votre application et capture un instantané de l'environnement entièrement initialisé.
3. Lorsque votre application a besoin d'un environnement isolé, pour une session utilisateur, une tâche ou un bac à sable, vous appelez`run-microvm`. Lambda lance une microVM à partir du snapshot avec des temps de démarrage rapides.
4. Les clients se connectent à la microVM en cours d'exécution via son point de terminaison HTTPS dédié. Aucun équilibreur de charge ou infrastructure d'entrée n'est requis.
5. Lorsqu'elle est inactive, la microVM s'arrête, préservant ainsi la mémoire et l'état du disque tout en réduisant les coûts. Il reprend avec la mémoire et l'état du disque intacts lorsque le trafic revient. Suspend-resume le comportement peut être configuré automatiquement par le biais de politiques de cycle de vie ou déclenché directement par des appels d'API à `suspend-microvm` et`resume-microvm`.
6. À la fin de la session, vous arrêtez la microVM pour libérer toutes les ressources.

Quand utiliser Lambda MicroVMS

Lambda MicroVMS convient parfaitement aux cas d'utilisation qui exécutent des utilisateurs ou du AI-generated code et nécessitent des environnements d'exécution offrant une isolation renforcée, une latence de lancement et de reprise rapides, et un contrôle des développeurs sur le cycle de vie de l'environnement et la conservation de l'état. Les cas d'utilisation typiques incluent :

- Environnements de code interactifs : environnements de développement dans lesquels les utilisateurs écrivent et exécutent du code en temps réel.
- Bacs à sable d'exécution de code IA — Bacs à sable éphémères pour exécuter du code en toute sécurité. AI-generated
- Applications d'analyse de données : blocs-notes Jupyter et charges de travail de traitement de données éphémères qui exécutent des scripts fournis par l'utilisateur.
- Analyse de sécurité : outils d'évaluation des vulnérabilités nécessitant des environnements d'exécution isolés.
- Environnements d'apprentissage renforcés : des bacs à sable isolés pour l'évaluation et la formation des agents d'IA, dans lesquels de nouveaux environnements sont créés à chaque exécution.
- Multi-tenant CI/CD— Exécuteurs de tâches nécessitant une isolation entre les locataires.

- Serveurs de jeux : environnements d'hébergement qui exécutent des scripts fournis par les utilisateurs avec une isolation renforcée.

Fonctionnalités principales

- Démarrage rapide : les micromachines virtuelles reprennent leurs activités à partir d'instantanés préinitialisés, en ignorant l'initialisation de l'application. Consultez Images microVM.
- Contrôle du cycle de vie : suspendez, reprenez et arrêtez les micromachines virtuelles par programmation ou automatiquement grâce à des politiques d'inactivité configurables. Consultez Exécution de microVMS.
- Réseau flexible : les micromachines virtuelles prennent en charge le trafic HTTPS entrant sur des ports configurables, avec une authentification JWE fournie par le service. L'accès sortant est configurable. Accédez à l'Internet public ou à votre VPC. Pour plus de détails, consultez le chapitre surMise en réseau.
- Allocation flexible des ressources : configurez chaque microVM pour une utilisation de référence ou moyenne, avec la flexibilité d'une mise à l'échelle verticale jusqu'à 4 fois la valeur de référence configurée pendant les pics d'activité. Payez le tarif de base pendant que votre microVM fonctionne et ne payez que pour une utilisation active supérieure au tarif de base.

AWS Lambda Concepts fondamentaux de MicroVMS

AWS Lambda MicroVMS utilise plusieurs types de ressources que vous créez et gérez. Cette page décrit chaque type de ressource, la manière dont Lambda crée votre image microVM en un instantané et le cycle de vie indique la transition d'une microVM au moment de l'exécution, ce qui constitue la base de la création d'applications avec MicroVMS.

Concepts clés

microVM

Une microVM est une ressource qui représente un environnement informatique isolé pour un locataire, une session utilisateur ou une tâche unique. Chaque microVM exécute un système d'exploitation Amazon Linux 2023 doté de fonctionnalités de système d'exploitation, permettant un lancement et une reprise quasi instantanés. Les micromachines virtuelles reçoivent des demandes via des connexions HTTPS entrantes et peuvent être suspendues lorsqu'elles sont

inactives, préservant ainsi la mémoire et l'état du disque. Une microVM suspendue reprend lorsque le trafic revient.

Image microVM

Une image microVM est une ressource qui définit l'environnement d'application d'une microVM. Lorsque vous créez une image, Lambda l'intègre dans un instantané qui permet un lancement quasi instantané (voir Comment Lambda construit votre image ci-dessous).

Pour créer une image microVM, vous devez fournir un package zip contenant un `Dockerfile` et les artefacts de votre application, chargés sur Amazon S3. Vous devez utiliser une image de base Lambda-published gérée comme base. Spécifiez-la à l'aide du `base-image-arn` paramètre. Your `Dockerfile` définit les couches d'application que Lambda construit au-dessus de la base gérée.

Les images MicroVM sont versionnées. Chaque version représente une construction unique produite à partir d'un artefact de code et d'une image de base spécifiques. Une version passe par les états de construction (`PENDING`→ `IN_PROGRESS` → `SUCCESSFUL` ou`FAILED`), et les versions réussies peuvent être définies sur `ACTIVE` ou`INACTIVE`. Pour plus de détails sur l'état et la gestion des images, consultezImages microVM.

Connecteurs réseau

Les connecteurs réseau sont des ressources qui contrôlent la manière dont le trafic atteint votre microVM et la manière dont votre microVM atteint les services externes. Vous associez des connecteurs à une microVM au moment de l'exécution pour configurer l'accès entrant et sortant indépendamment.

Build-time et les connecteurs d'exécution peuvent varier, ce qui permet à votre microVM d'accéder à différents environnements lors de la création de l'image par rapport à l'exécution.

Utilisez les Lambda-provided valeurs par défaut pour l'accès au port entrant (avec authentification JWE), l'accès au shell et la sortie Internet publique. Créez votre propre connecteur réseau pour acheminer le trafic sortant via votre VPC.

Comment Lambda construit votre image

Lorsque vous créez ou mettez à jour une image microVM, Lambda exécute un processus de génération qui produit un instantané Firecracker. Cet instantané capture l'état complètement initialisé de votre application, permettant un lancement et une reprise quasi instantanés pour les micromachines virtuelles qui s'exécutent à partir de celle-ci.

Le processus de création :

1. Lambda provisionne une nouvelle microVM à l'aide de l'image de base gérée que vous avez spécifiée.
2. Lambda exécute vos `Dockerfile` instructions pour installer les dépendances et configurer votre environnement.
3. Lambda démarre votre application à l'aide de la `CMD` commande `ENTRYPOINT` ou.
4. Si vous avez activé le `/ready` hook, Lambda attend que votre application signale qu'elle est prête (HTTP 200).
5. Lambda capture un instantané de l'état du disque et de la mémoire, y compris de tous les processus en cours d'exécution.

Lorsque vous exécutez une microVM, Lambda la restaure à partir de ce snapshot. Votre application reprend son état préinitialisé sans recommencer le démarrage.

Si votre application génère un contenu unique pendant la génération (tel que des identifiants uniques, des secrets ou des connexions réseau), ce contenu est partagé entre toutes les microVM exécutées à partir de la même version d'image. Pour éviter cela, générez un contenu unique une fois que la microVM a commencé à utiliser le hook du `/run` cycle de vie. Pour plus de détails, consultez la section sur la compatibilité des snapshots dansImages microVM.

Cycle de vie de la microVM

Au moment de l'exécution, une microVM passe par les étapes suivantes :

1. Courez — Vous appelez`run-microvm`. Lambda restaure la microVM à partir de la capture d'image, attribue un identifiant unique et crée un point de terminaison. La microVM passe de `PENDING` à. `RUNNING`
2. En cours d'exécution : votre application reçoit et traite les demandes via l'URL de son point de terminaison.
3. Suspendre : après une période d'inactivité configurable (ou via l'`suspend-microvm`API), la microVM passe `SUSPENDING` à`SUSPENDED`. L'état de la mémoire et du disque est préservé.
4. Reprise : la microVM passe du mode retour `SUSPENDED` direct au `RUNNING` moment où le trafic arrive (si`autoResumeEnabled=true`) ou lorsque vous appelez`resume-microvm`.
5. Terminer : la microVM passe `TERMINATING` au `TERMINATED` moment où vous appelez `terminate-microvm` ou lorsque la durée maximale est dépassée.

States

Le tableau suivant décrit l'état de chaque microVM. Ces états vous permettent de créer des applications fiables et de mettre en œuvre une gestion des erreurs appropriée.

State	Description
`PENDING`	La microVM est en cours de provisionnement. Les ressources sont allouées et le snapshot est en cours de chargement.
`RUNNING`	MicroVM est active et accepte le trafic via l'URL de son point de terminaison. Le `/run` crochet est terminé.
`SUSPENDING`	MicroVM est en cours de suspension. Le `/suspend` hook est en cours d'exécution. Le disque et la mémoire sont en cours de vérification.
`SUSPENDED`	MicroVM est suspendu. L'État est préservé. Aucun frais de calcul n'est facturé. Peut être repris ou résilié.
`TERMINATING`	MicroVM est en cours de fermeture. Le `/terminate` hook est en cours d'exécution. Les ressources sont en cours de publication.
`TERMINATED`	MicroVM a été arrêtée. Il s’agit d’un statut de terminal. La microVM ne peut pas être reprise ou redémarrée.

Transitions d'état

Le tableau suivant indique les transitions valides entre les états de la microVM et indique ce qui déclenche chaque transition.

Initial state (État initial)	État cible	Déclencheur
`PENDING`	`RUNNING`	L'approvisionnement est terminé, le `/run` crochet a réussi.
`RUNNING`	`SUSPENDING`	Durée d'inactivité dépassée ou appel `suspend-microvm` d'API explicite.

Initial state (État initial)	État cible	Déclencheur
SUSPENDING	SUSPENDED	/suspendcrochet terminé, contrôle de l'état de la mémoire et du disque.
SUSPENDED	RUNNING	Le trafic arrive (autoResumeEnabled= true) ou appelle explicitement resume-microvm l'API.
RUNNING	TERMINATING	Appel terminate-microvm d'API explicite , ou maximumDurationInSeconds dépassé.
SUSPENDED	TERMINATING	suspendedDurationSeconds dépassé ou appel d'terminate-microvm API explicite.
TERMINATING	TERMINATED	/terminate crochet terminé, toutes les ressources libérées.

> **Important**
>
> Si votre /run hook échoue ou expire, la microVM peut passer directement à TERMINATING sans jamais l'atteindreRUNNING. Implémentez la gestion des délais et des erreurs dans vos hooks pour éviter les défaillances silencieuses.

Créez votre première microVM Lambda

Ce didacticiel vous explique comment créer une image AWS Lambda microVM et exécuter une microVM à partir de celle-ci. À la fin, vous aurez une application en cours d'exécution accessible via HTTPS.

Conditions préalables

Vous avez besoin de deux choses avant de commencer :

1. Un compartiment Amazon S3 dans votre AWS région préférée pour stocker l'artefact de votre application (le fichier zip que vous allez créer à l'étape 2).
2. Un rôle de génération IAM que Lambda assume lors de la création de l'image. Lambda utilise ce rôle pour télécharger votre artefact de code depuis Amazon S3 et y écrire des journaux de génération. CloudWatch

Créez le rôle IAM avec la politique de confiance suivante. Cela permet au service Lambda de jouer le rôle suivant :

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Principal": { "Service": "lambda.amazonaws.com" },
    "Action": ["sts:AssumeRole", "sts:TagSession"]
  }]
}
```

Associez la politique d'autorisations suivante au rôle. Remplacez `<your-bucket-name>` par le nom de votre compartiment Amazon S3 :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["s3:GetObject"],
      "Resource": "arn:aws:s3:::<your-bucket-name>/*"
    },
    {
      "Effect": "Allow",
      "Action": ["logs:CreateLogGroup", "logs:CreateLogStream", "logs:PutLogEvents"],
      "Resource": "arn:aws:logs:*:*:*"
    }
  ]
}
```

> **Note**
>
> Si vous `Dockerfile` extrayez des données à partir d'un référentiel AWS ECR privé, ajoutez également « `ecr:GetAuthorizationToken` et » `ecr:BatchGetImage` à la politique d'autorisations.

Création de votre première image microVM

Une image microVM capture votre application dans un état complètement initialisé. Lorsque vous exécutez une microVM à partir de cette image, votre application démarre immédiatement, sans délai de démarrage ni d'initialisation.

Étape 1 : Rédigez votre application et Dockerfile

Créez un serveur HTTP simple qui s'exécute dans votre microVM. Cet exemple utilise Node.js sans dépendances externes :

`app.js`

```
// Minimal HTTP server — listens on port 8080
const http = require('http');

const server = http.createServer((req, res) => {
  res.writeHead(200, { 'Content-Type': 'application/json' });
  res.end(JSON.stringify({ status: 'ok', path: req.url }));
});

server.listen(8080, () => {
  console.log('Listening on port 8080');
});
```

Ensuite, créez un `Dockerfile` package et démarrez votre application :

`Dockerfile`

```
# Use a lightweight Node.js runtime for your application layers
FROM node:24-alpine

# Set the working directory inside the container
WORKDIR /app
```

```
# Copy your application code
COPY app.js .

# Declare the port your app listens on
EXPOSE 8080

# Start the application — Lambda snapshots the running state
CMD ["node", "app.js"]
```

> **Note**
>
> L'`FROM`instruction définit l'image du conteneur pour les couches de votre application. Vous pouvez utiliser n'importe quelle image de conteneur compatible. L'image de base gérée Lambda (qui fournit le système d'exploitation MicroVM et les composants de service) est spécifiée séparément `--base-image-arn` à l'étape 3.
>
> Si votre application génère des valeurs uniques (identifiants, secrets ou matériel cryptographique), utilisez la bibliothèque CSPRNG (cryptographiquement secure pseudorandom number generator) standard de votre langage pour garantir l'unicité sur toutes les microVM. Si votre application utilise OpenSSL, utilisez l'image du conteneur de base Lambda qui inclut une version compatible avec les snapshots. Pour plus de détails, consultez la section sur la compatibilité des snapshots dansImages microVM.

Étape 2 : empaqueter et charger sur Amazon S3

`app.js`Emballez votre `Dockerfile` annonce dans une archive zip, puis téléchargez-la dans votre compartiment Amazon S3. Exécutez les commandes suivantes dans votre terminal :

```
zip app.zip app.js Dockerfile
aws s3 cp app.zip s3://your-bucket-name/app.zip
```

Étape 3 : Création de l'image MicroVM

Appelez `create-microvm-image` pour démarrer la construction. Lambda télécharge votre fichier zip depuis Amazon S3, l'exécute`Dockerfile`, démarre votre application et capture un instantané de Firecracker à l'état complètement initialisé :

```
aws lambda-microvms create-microvm-image \
  --name my-first-microvm-image \
```

```
  --code-artifact uri=s3://your-bucket-name/app.zip \
  --base-image-arn arn:aws:lambda:us-east-1:aws:microvm-image:al2023-1 \
  --build-role-arn arn:aws:iam::123456789012:role/MicrovmBuildRole
```

L'image commence dans `CREATING` cet état. Vérifiez l'état de la construction avec :

```
aws lambda-microvms get-microvm-image \
  --image-identifier my-first-microvm-image
```

Une fois la génération terminée, le `state` champ devient `CREATED` :

```
{
  "imageName": "my-first-microvm-image",
  "imageArn": "arn:aws:lambda:us-east-1:123456789012:microvm-image:my-first-microvm-
image",
  "state": "CREATED",
  "imageVersion": "1.0",
  ...
}
```

Si c'est le cas`CREATE_FAILED`, vérifiez les journaux de compilation CloudWatch ci-dessous`/aws/lambda-microvms/my-first-microvm-image`.

Exécution de votre première microVM

Une fois que votre image MicroVM atteint son `CREATED` état, vous pouvez exécuter MicroVMS à partir de celle-ci. Chaque image peut lancer de nombreuses micromachines virtuelles, une par locataire, session utilisateur ou tâche.

Exécutez une microVM à l'aide de la commande suivante :

```
aws lambda-microvms run-microvm \
  --image-identifier my-first-microvm-image \
  --ingress-network-connectors "arn:aws:lambda:us-east-1:aws:network-connector:aws-
network-connector:ALL_INGRESS" \
  --egress-network-connectors "arn:aws:lambda:us-east-1:aws:network-connector:aws-
network-connector:INTERNET_EGRESS" \
  --idle-policy
 '{"autoResumeEnabled":true,"maxIdleDurationSeconds":900,"suspendedDurationSeconds":300}'
```

Paramètres expliqués :

- `--ingress-network-connectors`— Active le trafic HTTPS entrant vers votre microVM sur tous les ports. Il s'agit d'un Lambda-managed connecteur.
- `--egress-network-connectors`— Active l'accès Internet sortant depuis votre microVM. Il s'agit d'un Lambda-managed connecteur.
- `--idle-policy`— Configure le comportement automatique de suspension et de reprise. Cette politique suspend la microVM après 15 minutes d'inactivité, la maintient suspendue jusqu'à 5 minutes et reprend automatiquement à l'arrivée du trafic.

La réponse inclut l'ID de la microVM et l'URL du point de terminaison :

```
{
  "microvmId": "mvm-01234567-abcd-ef01-2345-6789abcdef01",
  "state": "PENDING",
  "endpoint": "mvm-01234567-abcd-ef01-2345-6789abcdef01.lambda-microvm.us-
east-1.on.aws",
  ...
}
```

Attendez que l'état atteigne `RUNNING` :

```
aws lambda-microvms get-microvm \
  --microvm-identifier mvm-01234567-abcd-ef01-2345-6789abcdef01
```

Connexion à votre microVM

Toutes les demandes adressées à un point de terminaison microVM nécessitent un jeton d'authentification. Générez-en un avec :

```
aws lambda-microvms create-microvm-auth-token \
  --microvm-identifier mvm-01234567-abcd-ef01-2345-6789abcdef01 \
  --expiration-in-minutes 30 \
  --allowed-ports '[{"allPorts":{}}]'
```

La réponse inclut un jeton dans le `authToken` champ. Utilisez-le pour envoyer une demande à votre application en cours d'exécution :

```
curl https://mvm-01234567-abcd-ef01-2345-6789abcdef01.lambda-microvm.us-east-1.on.aws/
 \
```

```
  -H "X-aws-proxy-auth: <token-value>"
```

Vous devriez voir la réponse de votre candidature :

```
{"status":"ok","path":"/"}
```

Votre microVM est en cours d'exécution et gère le trafic. L'application que vous avez écrite à l'étape 1 est disponible à l'URL du point de terminaison.

Nettoyage

Pour éviter des frais permanents, mettez fin à la microVM lorsque vous avez terminé :

```
aws lambda-microvms terminate-microvm \
  --microvm-identifier mvm-01234567-abcd-ef01-2345-6789abcdef01
```

Étapes suivantes

- Apprenez Concepts de base à comprendre le processus de capture d'écran, les états du cycle de vie et les images de base.
- Explorez Images microVM pour en savoir plus sur les hooks de création d'images, la gestion des versions et la compatibilité des snapshots.
- Consultez Exécution de microVMS des exemples de SDK, des hooks de cycle de vie et des stratégies de mise à l'échelle.
- Consultez the section called “Intégrations” les intégrations de services prises en charge.

Images de microVM

Cette section décrit comment créer, configurer, mettre à jour et gérer des images MicroVM.

Une image microVM est une ressource qui définit le système de fichiers et l'environnement d'application d'une microVM. L'image microVM inclut votre environnement d'exécution, le code de votre application et les programmes connexes tels que les processus d'arrière-plan et les agents d'observabilité. Pour créer une image microVM, vous devez fournir un package zip contenant un `Dockerfile` et les artefacts de votre application, que vous chargez sur Amazon S3.

Votre `Dockerfile` définit la manière dont votre application est empaquetée. Lambda crée l'image du conteneur de votre application en exécutant votre `Dockerfile` environnement au-dessus d'un

système d'exploitation fourni par une image de base Lambda-managed MicroVM. Les images de base de MicroVM sont décrites ci-dessous, dans la section intitulée —Images de base MicroVM.

Vous pouvez mettre à jour les images de base de votre microVM pour mettre à jour le code d'application ou la configuration de votre microVM. Chaque mise à jour que vous déclenchez crée une nouvelle version de l'image MicroVM.

Comment Lambda crée une image microVM

Lorsque vous créez une image microVM, Lambda :

- Récupère vos artefacts emballés depuis Amazon S3.
- Démarre une nouvelle microVM à partir de l'image de Lambda-managed base.
- Exécute les instructions de votre. `Dockerfile`
- Lance votre application à l'aide de l'`CMD`instruction `ENTRYPOINT` ou.
- Attend la fin de l'initialisation, signalée par votre hook de cycle de vie.
- Capture un instantané de l'état du disque et de la mémoire.

Une fois le processus de capture d'écran terminé, l'image de votre microVM entre dans l'`CREATED`état. Vous pouvez désormais utiliser cette image microVM pour créer une microVM, et chaque image microVM peut être utilisée pour créer plusieurs microVM indépendantes. Une microVM exécutée à partir de l'image microVM reprend directement à partir de l'état de capture instantanée, ce qui permet des temps de démarrage rapides. Chaque image microVM peut être utilisée pour exécuter plusieurs microVM, dans la limite disponible pour votre compte.

Pour une présentation étape par étape de l'empaquetage de votre code et de la création de votre première image microVM, reportez-vous à. Créez votre première microVM

Dimensionnement des microVM

Lambda MicroVMS utilise un modèle de pointe de référence qui élimine la nécessité de dimensionner correctement chaque environnement de calcul pour les pics d'activité. Vous configurez les ressources de calcul de base pour votre microVM. Pendant les pics d'activité, votre microVM peut automatiquement redimensionner verticalement jusqu'à 4 fois la valeur de référence. Vous payez le tarif de base pendant que votre microVM fonctionne et ne payez que pour ce que vous utilisez activement au-delà du niveau de référence, facturé à la seconde.

Vous définissez la référence à l'aide du `memory` paramètre lors de la création de votre image microVM. Le processeur virtuel évolue proportionnellement à la mémoire (2 Go = 1 processeur virtuel). La base de référence par défaut est de 2 Go/1 processeur virtuel.

Le tableau suivant répertorie les tailles disponibles :

Point de référence	Pic	Espace disque maximal
0,5 Go de mémoire, 0,25 vCPU	2 Go de mémoire, 1 processeur virtuel	8 Go
1 Go de mémoire, 0,5 vCPU	4 Go de mémoire, 2 processeurs virtuels	8 Go
2 Go de mémoire, 1 processeur virtuel (par défaut)	8 Go de mémoire, 4 processeurs virtuels	8 Go
4 Go de mémoire, 2 processeurs virtuels	16 Go de mémoire, 8 processeurs virtuels	16 Go
8 Go de mémoire, 4 processeurs virtuels	32 Go de mémoire, 16 processeurs virtuels	32 GO

Images de base MicroVM

Une image de base MicroVM sert de base à vos images MicroVM. Lambda publie une image de base MicroVM qui fournit le système d'exploitation Amazon Linux 2023 et les composants de service requis pour exécuter MicroVMS. Lorsque vous créez ou mettez à jour une image microVM, Lambda démarre une nouvelle microVM à partir de cette image de base et exécute vos `Dockerfile` instructions dans cet environnement de système d'exploitation.

Lambda publie régulièrement de nouvelles versions d'images de base de microVM gérées par des services, par exemple lors de l'application de correctifs de sécurité, pour mettre à jour le système d'exploitation ou les composants du service. Par défaut, la dernière version d'une image de base gérée par les services s'applique lorsque vous créez creating/updating vos propres images microVM. À des fins de dépannage ou de débogage, vous pouvez éventuellement remplacer la version des images basées sur les services gérés lors de la création de votre propre image microVM à l'aide du paramètre. `base-image-version`

Les versions des images de base suivent un cycle de vie obsolète :

- **AVAILABLE**— Actuel, utilisation recommandée.
- **DEPRECATED**(60 jours) — Une version plus récente existe. Vous pouvez toujours créer et exécuter.
- **EXPIRING**(30 jours) — Impossible de créer de nouvelles images. Les images existantes peuvent toujours s'exécuter.
- **EXPIRED**— Impossible de créer ou d'exécuter. Reconstruisez votre image sur une version prise en charge.
- **RECALLED**— Indisponible immédiatement en raison de problèmes de sécurité critiques (rare).

Pour rester à jour, surveillez les notifications d'obsolescence et reconstruisez vos images microVM lorsqu'une nouvelle version de l'image de base est publiée.

Notez que l'image de base de MicroVM est distincte de l'image de base du conteneur que vous spécifiez dans vos Dockerfiles. Alors que le premier définit l'environnement du système d'exploitation de vos micromachines virtuelles, le second définit l'image de conteneur de base à utiliser lors du packaging de votre application à utiliser avec des micromachines virtuelles Lambda. Pour en savoir plus, consultez la section sur Images de base de conteneur.

Utilisez les API suivantes pour découvrir les images de base de microVM gérées disponibles et leurs versions :

```
# List all managed MicroVM base images
aws lambda-microvms list-managed-microvm-images

# List the versions of a specific managed MicroVM base image
aws lambda-microvms list-managed-microvm-image-versions \
  --image-identifier arn:aws:lambda:us-east-1:aws:microvm-image:al2023-1
```

Hooks de création d'images MicroVM

Lambda fournit des crochets de génération d'images MicroVM qui vous permettent de vérifier l'exactitude des applications et d'optimiser les performances lors de la création d'images MicroVM. Les hooks s'exécutent avant que Lambda ne prenne le snapshot utilisé pour initialiser chaque microVM. Chaque hook est un point de terminaison HTTP que votre application expose et que Lambda appelle pendant la génération. En répondant à ces demandes, vous contrôlez et validez le processus de création d'images MicroVM. Lambda utilise des codes d'état HTTP pour déterminer si les hooks ont été correctement exécutés.

> **Important**
>
> Si vous configurez des hooks, vous devez spécifier le port sur lequel votre application écoute les demandes de hook.

Crochet	Chemin	Détails	Codes d'état HTTP	Timeout
/prêt	`/aws/lambda-microvms/runtime/v1/ready`	Appelé lors de la création de l'image MicroVM, après le démarrage de votre application via `ENTRYPOINT` ou`CMD`. Indique que votre application est prête à être capturée.	HTTP 503 : pas encore prêt ; Lambda réessaie jusqu'à l'expiration du délai imparti. HTTP 200 : initialisation terminée ; Lambda prend le cliché.	1 à 3 600 secondes () `readyTimeoutInSeconds`
/ valider	`/aws/lambda-microvms/runtime/v1/validate`	Appelé une fois la compilation terminée, sur une nouvelle microVM démarrée à partir de l'image créée. Confirme que l'application fonctionne correctement à la reprise.	HTTP 503 : la validation a besoin de plus de temps pour se terminer ; Lambda réessaie jusqu'à l'expiration du délai imparti. HTTP 200 : Validation réussie.	1 à 3 600 secondes () `validateTimeoutInSeconds`

> **Important**
>
> Lorsque vous renvoyez le protocole HTTP 503, renvoyez-le immédiatement plutôt que de maintenir la demande ouverte pendant que vous attendez. Si le délai d'attente expire alors qu'une requête est maintenue ouverte, Lambda met fin à la génération.

> **Note**
>
> Vous pouvez également utiliser le hook /validate pour optimiser le temps de démarrage. Pour ce faire, exécutez des charges utiles fictives lors de la validation. Cela permet à Lambda de suivre les régions consultées de votre instantané et d'optimiser leur récupération lors du démarrage de la microVM.

Mise à jour d'une image MicroVM

Vous pouvez mettre à jour une image microVM existante en appelant l'`update-microvm-image`API. Chaque mise à jour déclenche la création d'une nouvelle version de l'image MicroVM. Vous mettez généralement à jour une image microVM pour :

- Déployez le nouveau code d'application : pointez sur un nouvel artefact de code (un nouveau zip chargé sur Amazon S3) pour expédier une nouvelle version de votre application.
- Passer à une image de base MicroVM plus récente : modifiez l'ARN de l'image de base MicroVM pour passer à des versions plus récentes de l'image de base Lambda MicroVM. Pour plus d'informations, consultez Correctifs d'images sur microVM et Images de base MicroVM.
- Modifier le rôle de génération : mettez à jour l'ARN du rôle de génération lorsque les autorisations dont Lambda a besoin pendant la génération changent, par exemple lorsque votre artefact de code est déplacé vers un autre compartiment Amazon S3 ou que vous commencez à le récupérer depuis un référentiel ECR privé.
- Ajustez la configuration d'exécution : modifiez les hooks, les variables d'environnement ou les fonctionnalités pour reconfigurer la manière dont votre image microVM est créée et exécutée.
- Mettre à jour la description — Modifiez la description de l'image MicroVM pour enregistrer les modifications apportées à cette version.

La commande CLI suivante montre comment mettre à jour une image microVM. Les `--build-role-arn` paramètres `--base-image-arn` et sont requis pour chaque `update-microvm-image` appel qui déclenche une nouvelle version, même lorsque vous ne modifiez que l'artefact de code. Les omettre entraîne : `ValidationException`

```
aws lambda-microvms update-microvm-image \
  --image-identifier arn:aws:lambda:us-east-1:123456789012:microvm-image:my-microvm-image \
  --code-artifact uri=s3://my-bucket/deployments/app-v2.zip \
```

```
  --base-image-arn arn:aws:lambda:us-east-1:aws:microvm-image:al2023-1 \
  --build-role-arn arn:aws:iam::123456789012:role/MicrovmBuildRole \
  --description "Updated with v2 application code"
```

États de l'image et états de construction

Chaque fois que vous créez ou mettez à jour une image microVM, Lambda produit une nouvelle version construite à partir de votre artefact de code et de votre image de base. Une image microVM peut avoir de nombreuses versions au fil du temps, et vous exécutez MicroVM à partir d'une version spécifique.

Trois États indépendants suivent différents aspects du cycle de vie :

- État de l'image : cycle de vie global de la ressource d'image MicroVM (en cours de création, prête à être utilisée, mise à jour, échec ou suppression).
- État de la version : progression de la génération d'une version spécifique (en attente, en cours de création, réussie ou échec). Vérifiez `stateReason` ou enregistrez CloudWatch (`/aws/lambda-microvms/<image-name>`) pour plus de détails sur les défaillances.
- Activation de la version : indique si une version créée avec succès est autorisée à exécuter des micromachines virtuelles. Lambda définit `ACTIVE` automatiquement les nouvelles versions ; vous pouvez définir une version `INACTIVE` pour la désactiver sans la supprimer.

State	Valeurs possibles	Transition contrôlée par
État de l'image	`CREATING`, `CREATED`, `CREATION_FAILED`, `UPDATING`, `UPDATED`, `UPDATE_FAILED`, `DELETING`, `DELETED`, `DELETION_FAILED`	Lambda (automatique)
État de la version	`PENDING`, `IN_PROGRESS`, `SUCCESSFUL`, `FAILED`	Lambda (automatique)
Activation de la version	`ACTIVE`, `INACTIVE`	Vous (`update-microvm-image-version --state`)

Pour exécuter une microVM à partir d'une version, l'état de l'image doit être `CREATED` ou`UPDATED`, l'état de la version doit être `SUCCESSFUL` et la version doit être`ACTIVE`.

> **Note**
>
> Ces États sont indépendants. Une image dans `CREATED` cet état peut contenir une version dont l'état est`FAILED`.

```
# De-activate a version
aws lambda-microvms update-microvm-image-version \
  --image-identifier my-image \
  --image-version 1.0 \
  --state INACTIVE
```

Variables d’environnement

Les variables d'environnement sont définies au moment de la création de l'image MicroVM `environmentVariables` dans le champ (50 variables maximum). Ils sont injectés dans le conteneur pendant le processus de création du snapshot. Vous pouvez transmettre des charges utiles définies dynamiquement lors de l'exécution d'une nouvelle microVM. Reportez-vous à la section sur l'exécution de votre microVM pour en savoir plus.

Utilisation des instantanés

Lorsque AWS Lambda MicroVMS crée une image MicroVM, il capture un instantané Firecracker de votre application entièrement initialisée. Cette page décrit le contenu d'un instantané, comment gérer l'unicité des microVM partageant le même instantané et les meilleures pratiques pour les applications compatibles avec les instantanés.

Ce qu'un instantané permet de capturer

Un instantané Firecracker capture l'état suivant à partir de votre microVM au moment où la création de l'image est terminée :

- État de la mémoire des processus en cours d'exécution : tous les processus lancés par`ENTRYPOINT`/`CMD`, y compris les démons d'arrière-plan, les tâches cron et les processus enfants.
- État du disque : système de fichiers racine, y compris tous les fichiers écrits pendant la phase de construction (packages installés, fichiers binaires compilés, fichiers de configuration).

- Connexions réseau et descripteurs de fichiers : toutes les connexions réseau, descripteurs de fichiers, canaux et autres descripteurs initialisés.

Lorsque vous exécutez une microVM, Lambda la restaure à partir de ce snapshot. Votre application reprend exactement là où la version de l'image MicroVM s'était arrêtée.

Considérations de compatibilité

Étant donné que toutes les microVM lancées à partir de la même version d'image partagent le même état initial, tenez compte des points suivants lorsque vous créez des applications avec Lambda MicroVMS :

- Unicité : si votre code génère un contenu unique pendant la phase de création de la version de l'image (ID uniques, secrets ou entropie pour le caractère pseudo-aléatoire), ce contenu est partagé entre toutes les microVM exécutées à partir de la même version d'image. Générez un contenu unique après le démarrage d'une nouvelle microVM, et non pendant la création de l'image. Utilisez le hook `/run` du cycle de vie pour réinitialiser le contenu unique généré précédemment.
- Connexions réseau : les connexions établies pendant la phase de création de la version de l'image peuvent devoir être rétablies lorsqu'une microVM est exécutée à partir de la version de l'image. Validez l'état de la connexion et rétablissez les connexions si nécessaire. Dans la plupart des cas, les connexions créées par AWS les SDK sont automatiquement rétablies.

Gérer l'unicité à l'aide des instantanés

Toutes les micromachines virtuelles exécutées à partir de la même image partagent le même état initial. Pour préserver l'unicité des micromachines virtuelles, procédez comme suit :

- Générez des identifiants uniques, des secrets et des valeurs aléatoires après le démarrage d'une microVM et non lors de la création de la version de l'image. Utilisez le hook `/run` du cycle de vie pour réinitialiser n'importe quel état unique.
- Utilisez des générateurs de nombres pseudo-aléatoires sécurisés sur le plan cryptographique (CSPRNG) pour votre langage de programmation. Vérifiez que votre bibliothèque cryptographique standard reçoit son entropie de l'appareil ou de l'`/dev/random`appareil. `/dev/urandom` Il s'agit du comportement par défaut pour les bibliothèques cryptographiques des langages de programmation courants tels que Java 11+ (SecureRandom bibliothèque), Node.js (bibliothèque Crypto.RandomBytes), Python 3.12+ (bibliothèque) et Dotnet8+ (Secrets.SystemRandombibliothèque). Cryptography.RandomNumberGenerator Logiciel qui lit

`/dev/random` ou `/dev/urandom` conserve le caractère aléatoire lorsqu'il est utilisé avec des instantanés d'images microVM.

- Si le code de votre application utilise OpenSSL, utilisez l'image de conteneur de base AWS fournie `public.ecr.aws/lambda/microvms:al2023-minimal` à partir de pour créer votre image microVM. Cette image contient une version AWS corrigée d'OpenSSL qui est compatible avec la capture instantanée. Si vous souhaitez utiliser votre propre image de base avec OpenSSL, utilisez la version corrigée d'OpenSSL (openssl-snapsafe-libs) répertoriée dans la liste des packages Amazon Linux 2023. https://docs.aws.amazon.com/linux/al2023/release-notes/all-packages.html

Correctifs d'images sur microVM

Lorsqu'une nouvelle image de base MicroVM est disponible, vous pouvez émettre un `update-microvm-image` appel pour déclencher la génération d'une image MicroVM avec les derniers correctifs, soit en omettant l'`base-image-version`argument (pour le plus récent), soit en spécifiant l'argument avec la dernière version.

Images de base de conteneur

Lambda MicroVMS exécute votre application en tant que conteneur dans l'environnement du système d'exploitation MicroVM. Vous définissez ce conteneur avec votre`Dockerfile`, et les `FROM` instructions qu'il contient `Dockerfile` définissent l'image de base du conteneur pour votre application.

Vous pouvez soit commencer par l'image du conteneur de base Lambda pour Amazon Linux 2023 (`public.ecr.aws/lambda/microvms:al2023-minimal`) et y ajouter vos `Dockerfile` instructions, soit utiliser votre propre image de conteneur de base. Lorsque vous utilisez vos propres images de conteneurs, validez les exigences suivantes :

Exigences

- L'image de base du conteneur doit être compatible avec l'architecture du processeur cible.
- Les images de base de conteneurs provenant de référentiels AWS ECR privés nécessitent le rôle de génération `ecr:GetAuthorizationToken` et `ecr:BatchGetImage` des autorisations.
- L'image de base du conteneur doit être basée sur un système d'exploitation Linux.
- Les images de base de conteneurs doivent être accessibles depuis l'infrastructure de compilation Lambda (Internet public ou référentiel ECR sur le même AWS compte).

- Les images de base du conteneur doivent être compatibles avec les captures d'écran, voir les instructions ci-dessous.

Snapshot-compatible images de base

Comme Lambda MicroVMS démarre chaque microVM à partir d'un instantané pré-initialisé, les images de base doivent être compatibles avec les instantanés. Nous vous recommandons de consulter la section relative à l'Considérations de compatibilitéutilisation de vos propres images de base avec Lambda MicroVMS.

Utilisation d'une image ECR privée

Faites référence à l'image de base de votre conteneur ECR privé dans les `FROM` instructions de votre `Dockerfile` :

```
FROM 123456789012.dkr.ecr.us-east-1.amazonaws.com/my-base:latest
WORKDIR /app
COPY . .
CMD ["./my-app"]
```

Ajoutez les autorisations suivantes à votre rôle de build :

```
{
  "Effect": "Allow",
  "Action": [
    "ecr:GetAuthorizationToken",
    "ecr:BatchCheckLayerAvailability",
    "ecr:GetDownloadUrlForLayer",
    "ecr:BatchGetImage"
  ],
  "Resource": "*"
}
```

Fonctionnalités du système d'exploitation

Par défaut, les micromachines virtuelles Lambda s'exécutent avec un ensemble standard de fonctionnalités Linux. Vous pouvez accorder des fonctionnalités Linux élevées à l'aide du `additionalOsCapabilities` champ lors de la création ou de la mise à jour d'une image microVM. La seule valeur prise en charge est `["ALL"]`. Les fonctionnalités avancées permettent des

opérations telles que le montage de systèmes de fichiers, la création d'espaces de noms réseau ou l'exécution de programmes eBPF. Les fonctionnalités sont appliquées dans les limites d'isolation de la machine virtuelle et n'affectent pas l'hôte ou les autres micromachines virtuelles.

```
aws lambda-microvms create-microvm-image \
  --name my-network-tool \
  --code-artifact uri=s3://my-bucket/app.zip \
  --base-image-arn arn:aws:lambda:us-east-1:aws:microvm-image:al2023-1 \
  --build-role-arn arn:aws:iam::123456789012:role/BuildRole \
  --additional-os-capabilities '["ALL"]'
```

Exécution et utilisation de microVMS

Cette section décrit comment démarrer des micromachines virtuelles, vous connecter à vos applications en cours d'exécution, gérer le cycle de vie des micromachines virtuelles et gérer la mise à l'échelle.

Démarrage d'une microVM

Utilisez la `run-microvm` commande pour lancer une nouvelle microVM à partir d'une image spécifiée. Lambda fournit les ressources nécessaires, crée un point de terminaison HTTPS dédié et démarre votre application à partir de l'instantané de l'image.

```
aws lambda-microvms run-microvm \
  --image-identifier arn:aws:lambda:us-east-1:123456789012:microvm-image:my-microvm-
image \
  --ingress-network-connectors "arn:aws:lambda:us-east-1:aws:network-connector:aws-
network-connector:ALL_INGRESS" \
  --egress-network-connectors "arn:aws:lambda:us-east-1:aws:network-connector:aws-
network-connector:INTERNET_EGRESS" \
  --idle-policy
 '{"autoResumeEnabled":true,"maxIdleDurationSeconds":900,"suspendedDurationSeconds":1800}'
 \
  --maximum-duration-in-seconds 14400
```

Une microVM est créée lorsque vous appelez`run-microvm`. Chaque microVM possède son propre point de terminaison dédié. Il n'y a pas d'équilibrage de charge entre les micromachines virtuelles à partir d'un seul point de terminaison : chaque point de terminaison est lié à une seule micromachine virtuelle.

Le seul paramètre obligatoire est `--image-identifier` (qui doit être l'ARN de l'image microVM). Tous les autres paramètres sont facultatifs.

Paramètres clés

Paramètre	Description
`--image-identifier`	(Obligatoire) L'ARN de l'image microVM à exécuter.
`--image-version`	Version de l'image microVM à exécuter. Par défaut, il s'agit de la dernière version active.
`--execution-role-arn`	Le rôle IAM qui fournit des autorisations d'exécution permettant à la microVM d'interagir avec d'autres AWS services.
`--idle-policy`	Contrôle le comportement de suspension et de reprise automatiques. Consultez la section suivante sur la configuration de la politique d'inactivité.
`--maximum-duration-in-seconds`	Durée de vie totale maximale de la microVM, y compris la durée de fonctionnement et la durée de suspension. Lambda arrête la microVM lorsque cette durée est dépassée. Plage : 1 à 28 800 secondes (8 heures).
`--run-hook-payload`	Une charge utile de chaîne (16 Ko maximum) envoyée au hook du `/run` cycle de vie au démarrage de la microVM.
`--logging`	Configuration de la journalisation. Personnalisez le groupe de CloudWatch journaux et le flux, ou désactivez complètement la journalisation.
`--ingress-network-connectors`	Les ARN des connecteurs d'entrée qui permettent la connectiv ité HTTPS entrante.
`--egress-network-connectors`	Le ou les ARN des connecteurs de sortie pour la connectivité sortante (Internet ou VPC).

> **Note**
>
> Pour désactiver la connectivité d'entrée, utilisez le Lambda-provided `NO_INGRESS` connecteur. Pour plus de détails sur les connecteurs réseau, consultezthe section called "Mise en réseau".

Configuration de la politique inactive

Lorsqu'elle est activée, la politique d'inactivité contrôle la suspension et la reprise automatiques. La présence de trafic via le terminal de la microVM signale une activité. Si aucun trafic n'arrive pendant la durée d'inactivité configurée, la microVM est considérée comme inactive et suspendue.

Champ	Description
`autoResumeEnabled`	Lorsque`true`, la microVM reprend automatiquement lorsque le trafic arrive à son point de terminaison alors qu'il est suspendu.
`maxIdleDurationSeconds`	Le nombre de secondes sans trafic après lesquelles la microVM est suspendue. Maximum : 28 800 (8 heures).
`suspendedDurationSeconds`	Le nombre de secondes pendant lesquelles une microVM reste à l'état suspendu avant que Lambda ne l'arrête.

> **Note**
>
> Pour les applications asynchrones qui n'envoient ou ne reçoivent pas activement de trafic via le terminal, désactivez la suspension automatique ou configurez une durée d'inactivité appropriée.

Charges utiles d'exécution

Avec `runHookPayload` ce paramètre, vous pouvez transmettre des données de configuration par microVM (chaîne de 16 Ko maximum) au moment de l'exécution. Lambda fournit cette charge utile dans le cadre du corps de la requête au hook du `/run` cycle de vie. Lambda injecte également le `microvmId` dans le corps de la requête.

Le `/run` hook reçoit un corps JSON dont la structure est la suivante :

```
{
  "microvmId": "mvm-01234567-abcd-ef01-2345-6789abcdef01",
  "runHookPayload": "tenant-specific-string"
}
```

Utilisez les charges utiles d'exécution pour fournir une configuration qui varie en fonction de la microVM, par exemple, les identifiants de locataire, les jetons de session, les URL signées ou les chemins du Secrets Manager. Contrairement aux variables d'environnement (qui sont définies au niveau de l'image et partagées entre toutes les microVM à partir de cette image), la charge utile du run hook est unique à chaque microVM.

```
aws lambda-microvms run-microvm \
  --image-identifier arn:aws:lambda:us-east-1:123456789012:microvm-image:my-microvm-image \
  --run-hook-payload 'tenant-specific-string'
```

Lorsque vous n'avez plus besoin d'une microVM, mettez-la hors service pour arrêter tous les frais. Pour obtenir des instructions, consultez the section called “Terminer une microVM”.

Connexion à une microVM

Chaque microVM reçoit une URL de point de terminaison HTTPS public unique, attribuée lorsque vous appelez`run-microvm`. Vous vous connectez à votre application exécutée dans la microVM via cette URL.

Authentification

Toutes les demandes adressées à un terminal microVM nécessitent un jeton d'authentification JWE. Il n'existe aucune option d'accès non authentifié. Générez un jeton avec `create-microvm-auth-token` :

```
aws lambda-microvms create-microvm-auth-token \
  --microvm-identifier microvm-id \
  --expiration-in-minutes 30 \
  --allowed-ports '[{"allPorts":{}}]'
```

Les jetons sont limités à des ports spécifiques et ont une expiration configurable. Vous pouvez restreindre l'accès à un seul port, à une plage de ports ou à tous les ports :

```
{ "port": number }
{ "range": { "startPort": N, "endPort": N } }
{ "allPorts": {} }
```

Routage des ports

Par défaut, Lambda achemine le trafic entrant vers le port 8080 de votre microVM. Pour acheminer vers un autre port, incluez l'`X-aws-proxy-port`en-tête dans votre demande. Le port cible doit se situer dans les limites `allowedPorts` définies dans le jeton d'authentification.

Protocoles

Lambda MicroVMS prend en charge HTTP/2 WebSockets, gRPC et SSE sur l'URL du point de terminaison.

Pour les WebSocket connexions, transmettez le jeton d'authentification et le port cible via des sous-protocoles :

```
// JavaScript WebSocket example
const protocols = [
  "lambda-microvms",                              // Required base protocol
  "lambda-microvms.authentication.<auth-token>",  // Auth token
  "lambda-microvms.port.9000"                     // Target port
];
const ws = new WebSocket('wss://<microvm-endpoint>/path', protocols);
```

Lambda supprime les MicroVM-specific sous-protocoles de la demande avant de la transmettre à votre application.

Exemples de SDK

Les exemples suivants montrent comment exécuter une microVM et s'y connecter à l'aide des AWS kits SDK.

Python

Example Exemple — Exécution d'une microVM et connexion avec boto3

```
import boto3, requests
```

```
client = boto3.client("lambda-microvms")
run_resp = client.run_microvm(
    imageIdentifier="arn:aws:lambda:us-east-1:123456789012:microvm-image:my-microvm-
image",
    idlePolicy={"autoResumeEnabled": True, "maxIdleDurationSeconds": 900,
 "suspendedDurationSeconds": 300}
)
microvm_id = run_resp["microvmId"]
endpoint = run_resp["endpoint"]
print(f"MicroVM {microvm_id} running at {endpoint}")
token_resp = client.create_microvm_auth_token(
    microvmIdentifier=microvm_id, expirationInMinutes=30, allowedPorts=[{"allPorts":
 {}}]
)
token = token_resp["authToken"]["X-aws-proxy-auth"]
resp = requests.get(f"https://{endpoint}/health", headers={"X-aws-proxy-auth":
 token})
print(resp.status_code, resp.json())
```

Node.js

Example Exemple — Exécution d'une microVM et connexion avec AWS SDK pour JavaScript

```
import { LambdaMicrovmsClient, RunMicrovmCommand, CreateMicrovmAuthTokenCommand }
 from "@aws-sdk/client-lambda-microvms";
const client = new LambdaMicrovmsClient({});
const { microvmId, endpoint } = await client.send(new RunMicrovmCommand({
  imageIdentifier: "arn:aws:lambda:us-east-1:123456789012:microvm-image:my-microvm-
image",
  idlePolicy: { autoResumeEnabled: true, maxIdleDurationSeconds: 900,
 suspendedDurationSeconds: 300 }
}));
const { authToken } = await client.send(new CreateMicrovmAuthTokenCommand({
  microvmIdentifier: microvmId, expirationInMinutes: 30, allowedPorts: [{ allPorts:
 {} }]
}));
const resp = await fetch(`https://${endpoint}/health`, {
  headers: { "X-aws-proxy-auth": authToken["X-aws-proxy-auth"] }
});
console.log(await resp.json());
```

Envoi de demandes

Bash

Example Exemple — Envoi d'une demande avec cURL

```
curl 'https://<microvm-endpoint>' \
  -H 'X-aws-proxy-auth: <TOKEN>' \
  -H 'X-aws-proxy-port: 8080'
```

Python

Example Exemple — Envoi d'une demande avec la bibliothèque de requêtes

```
import requests
response = requests.get('https://<microvm-endpoint>', headers={'X-aws-proxy-auth':
 '<TOKEN>'})
print(response.text)
```

Node.js

Example Exemple — Envoi d'une requête avec fetch

```
const response = await fetch('https://<microvm-endpoint>', {
  headers: { 'X-aws-proxy-auth': '<TOKEN>', 'X-aws-proxy-port': '8080' }
});
console.log(await response.text());
```

Hooks de cycle de vie

Les hooks de cycle de vie vous permettent d'exécuter une logique personnalisée à des moments clés du cycle de vie de la microVM : lors de son démarrage, de sa suspension, de sa reprise ou de son arrêt. Utilisez des hooks pour initialiser l'état par locataire, vider les données avant la suspension, actualiser les informations d'identification à la reprise ou nettoyer les ressources avant la résiliation.

Chaque hook est un point de terminaison HTTP exposé par votre application. Lambda envoie une requête POST au hook lors de l'événement de cycle de vie approprié. Les hooks écoutent le chemin `/aws/lambda-microvms/runtime/v1/<hook-name>` du port que vous configurez.

Votre microVM commence à recevoir du trafic externe une fois que le `/run` hook a renvoyé HTTP 200. D'ici là, le terminal ne transmet pas les demandes à votre application.

Crochet	Lorsqu'il est invoqué	Objectif
`/aws/lambda-microvms/runtime/v1/run`	Après le démarrage de MicroVM à partir d'un instantané	Initialisez l'état par locataire, réinitialisez les valeurs uniques, effectuez des contrôles de santé. Le trafic commence après le retour de ce hook.
`/aws/lambda-microvms/runtime/v1/resume`	Après la reprise de l'état suspendu de MicroVM	Re-establish connexions réseau, actualisation des informations d'identification, validation de l'état. La microVM reste en `SUSPENDED` état pendant l'exécution de ce hook ; elle passe `RUNNING` après le retour du hook.
`/aws/lambda-microvms/runtime/v1/suspend`	Avant la suspension de MicroVM	Videz les écritures en attente, fermez les connexions, libérez des ressources.
`/aws/lambda-microvms/runtime/v1/terminate`	Avant l'arrêt de MicroVM	Videz les données, notifiez les systèmes externes, nettoyez. Ce crochet ne fonctionne qu'en cas de terminaison définitive, pas lors de la suspension. Utilisez le `/suspend` crochet pour le nettoyage avant la suspension.

Pour les hooks qui s'exécutent lors de la création de l'image (`/ready`et`/validate`), consultezHooks de création d'images MicroVM.

Spécification OpenAPI :

```
{
  "openapi": "3.0.2",
  "info": {
    "title": "Lambda MicroVMs Application Hook Interface",
    "version": "2025-12-03"
  },
  "paths": {
    "/ready": {
      "post": {
        "description": "Called by Lambda during MicroVM image creation to determine if
 the application has initialized.",
```

```
        "operationId": "Ready",
        "responses": {
          "200": { "description": "Successful invocation." },
          "503": { "description": "Application is not yet ready. Lambda retries until
timeout." }
        }
      }
    },
    "/resume": {
      "post": {
        "description": "Called by Lambda when resuming a MicroVM that is in the
SUSPENDED state.",
        "operationId": "Resume",
        "responses": {
          "200": { "description": "Successful invocation." }
        }
      }
    },
    "/run": {
      "post": {
        "description": "Called by Lambda when a new MicroVM is run from a MicroVM
image.",
        "operationId": "Run",
        "requestBody": {
          "content": {
            "application/json": {
              "schema": { "$ref": "#/components/schemas/RunRequestContent" }
            }
          }
        },
        "responses": {
          "200": { "description": "Successful invocation." }
        }
      }
    },
    "/suspend": {
      "post": {
        "description": "Called by Lambda when suspending a MicroVM.",
        "operationId": "Suspend",
        "responses": {
          "200": { "description": "Successful invocation." }
        }
      }
    },
```

```
    "/terminate": {
      "post": {
        "description": "Called by Lambda when terminating a MicroVM, before resources
are released.",
        "operationId": "Terminate",
        "responses": {
          "200": { "description": "Successful invocation." }
        }
      }
    },
    "/validate": {
      "post": {
        "description": "Called by Lambda when running a MicroVM to validate the
image build. Use this hook to perform tests that validate your application behaves
correctly when running. Lambda also samples the portions of the image that are used
when handling this request, allowing Lambda to prefetch those portions of the image to
reduce latency at run time.",
        "operationId": "Validate",
        "responses": {
          "200": { "description": "Successful invocation." },
          "503": { "description": "Validation in progress. Lambda retries until
timeout." }
        }
      }
    }
  },
  "components": {
    "schemas": {
      "RunRequestContent": {
        "type": "object",
        "properties": {
          "microvmId": {
            "type": "string",
            "description": "The MicroVM identifier."
          },
          "runHookPayload": {
            "type": "string",
            "description": "Run hook payload provided to RunMicrovm."
          }
        }
      }
    }
  },
  "servers": [
```

```
    { "url": "/aws/lambda-microvms/runtime/v1" }
  ]
}
```

Suspension et reprise des microVM

Suspendez les micromachines virtuelles pour réduire les coûts tout en préservant l'état de l'application. Pendant que vous courez, vous payez des frais de calcul. Pendant la suspension, vous ne payez que les frais de stockage des instantanés.

Comment suspendre

Il existe deux manières de suspendre une microVM :

1. Politique d'inactivité (automatique) — Configurez `maxIdleDurationSeconds` dans la politique d'inactivité. Si aucun trafic n'arrive au point de terminaison de la microVM pendant cette durée, Lambda suspend automatiquement la microVM.
2. Appel d'API (explicite) — Appel `suspend-microvm` à suspendre immédiatement :

```
aws lambda-microvms suspend-microvm --microvm-identifier microvm-id
```

Le crochet /suspend

Avant de suspendre, Lambda appelle votre `/suspend` hook. Utilisez-le pour vider les écritures en attente, fermer les connexions réseau et libérer les ressources qui ne doivent pas persister au-delà de la limite de suspension.

Comportement du CV

Lorsqu'une microVM redémarre (via un appel d'API ou une reprise automatique), Lambda restaure la mémoire et l'état du disque à partir du point de contrôle de suspension. La microVM reste en `SUSPENDED` état pendant l'exécution du `/resume` hook. Une fois que le hook a renvoyé HTTP 200, la microVM passe au trafic `RUNNING` et commence à recevoir du trafic.

Utilisez le `/resume` hook pour actualiser les informations d'identification, rétablir les connexions réseau et valider l'état.

```
aws lambda-microvms resume-microvm --microvm-identifier microvm-id
```

Auto-resume

Lorsque `autoResumeEnabled=true` le trafic arrive au point de terminaison d'une microVM suspendue, Lambda la relance automatiquement. Lambda conserve la demande entrante pendant que le CV est terminé (y compris le `/resume` hook), puis la transmet à votre candidature.

Le CV ajoute de la latence à la première demande. La durée dépend de l'ampleur de l'état suspendu en cours de restauration et de la durée de votre `/resume` hameçon.

Si la reprise échoue, Lambda renvoie le 502 Bad Gateway à l'appelant.

> **Note**
>
> Auto-resume ajoute de la latence uniquement à la première demande après la suspension. Les requêtes suivantes pendant l'exécution de la microVM ne sont pas affectées.

Mise à l'échelle et simultanéité

Vous créez de nouvelles micromachines virtuelles en appelant. `run-microvm` Chaque microVM possède son propre point de terminaison dédié. Il n'y a pas d'équilibrage de charge entre les microVM à partir d'un seul point de terminaison.

Account-level capacité : votre compte dispose d'un quota pour la mémoire totale qui peut être allouée à toutes vos micromachines virtuelles dans l'`SUSPENDED`état `RUNNING` ou d'une région, et vous pouvez le redimensionner verticalement jusqu'à quatre fois ce quota. Pour demander une augmentation de quota, accédez à la console Service Quotas et recherchez Lambda MicroVMS.

Modèle de coût :

- L'exécution de microVM entraîne des frais de calcul.
- Les micromachines virtuelles suspendues entraînent des frais de stockage des snapshots, mais pas des frais de calcul.
- Les micromachines virtuelles résiliées n'entraînent aucun frais.

Stratégies de gestion des capacités :

- Suspendre les micromachines virtuelles inactives : configurez des politiques d'inactivité pour suspendre automatiquement les micromachines virtuelles qui ne reçoivent pas de trafic.

- Mettre fin aux micromachines virtuelles qui ne sont plus nécessaires : utilisez cette option `suspendedDurationSeconds` pour terminer automatiquement après une durée de suspension maximale, ou appelez explicitement. `terminate-microvm`
- Right-size politiques d'inactivité : définissez `maxIdleDurationSeconds` en fonction de vos habitudes de trafic. Des temps d'inactivité plus courts permettent de libérer de la capacité plus rapidement.

Terminer une microVM

Arrêtez une microVM lorsqu'elle n'est plus nécessaire. La résiliation libère toutes les ressources de calcul et met fin à tous les frais.

Avant de publier des ressources, Lambda appelle votre `/terminate` hook. Utilisez-le pour vider les données en attente ou avertir les systèmes externes. Le `/terminate` hook ne s'exécute que lors de la terminaison finale ; il ne s'exécute pas lorsqu'une microVM est suspendue.

```
aws lambda-microvms terminate-microvm --microvm-identifier microvm-id
```

Répertorier les microVM

Répertoriez toutes les micromachines virtuelles de votre compte, éventuellement filtrées par image :

```
aws lambda-microvms list-microvms

# Filter by image
aws lambda-microvms list-microvms --image-identifier my-image --image-version 1.0
```

Gestion des erreurs

Erreurs d'exécution

Le tableau suivant répertorie les erreurs courantes renvoyées par l'`run-microvm`API :

Erreur	Cause	Solution
`ServiceQuotaExceededException`	Le compte a atteint son quota de mémoire pour les micromach	Mettez fin aux micromachines virtuelles inactives ou demandez une augmentation de quota.

Erreur	Cause	Solution
	ines virtuelles simultanées.	
`ResourceNotFoundException`	L'image spécifiée n'existe pas ou n'est pas dans son `CREATED` état.	Vérifiez l'identifiant de l'image et confirmez que la création est terminée.
`ValidationException`	Un ou plusieurs paramètres de demande ne sont pas valides.	Vérifiez les valeurs de politique d'inactivité, le format de l'identifiant d'image et les ARN des connecteurs.
`ThrottlingException`	La limite de débit de l'API pour cette opération a été dépassée.	Implémentez un ralentissement exponentiel avec gigue.

Stratégie de nouvelle tentative

Pour les erreurs transitoires (`ThrottlingException`,`InternalServerException`), utilisez un retard exponentiel :

```
import time, random
def run_with_retry(client, params, max_retries=5):
    for attempt in range(max_retries):
        try:
            return client.run_microvm(**params)
        except client.exceptions.ThrottlingException:
            delay = (2 ** attempt) + random.uniform(0, 1)
            time.sleep(delay)
    raise Exception("Max retries exceeded")
```

Pour plus d'informations sur les intégrations de services prises en charge avec les instances gérées Lambda, consultez. the section called “Intégrations”

Mise en réseau

Vous configurez l'accès réseau pour vos AWS Lambda microVM en associant les ressources du connecteur réseau à votre microVM au moment de l'exécution. Les connecteurs réseau sont spécifiés lorsque vous appelez `run-microvm` et ne peuvent pas être modifiés lorsqu'une microVM est en cours d'exécution.

Vue d’ensemble

Chaque microVM peut avoir des configurations réseau d'entrée (entrante) et de sortie (sortante) indépendantes :

- Les connecteurs réseau d'entrée permettent la connectivité entrante. Les clients se connectent à un point de terminaison HTTPS géré par un service, et Lambda transmet le trafic aux ports que vous configurez au sein de la microVM. Les connecteurs d'entrée sont AWS gérés : vous les référencez par ARN lorsque vous exécutez une microVM.
- Les connecteurs réseau de sortie permettent le trafic sortant. Par défaut, les microVM disposent d'un accès public à Internet. Vous pouvez créer un connecteur de sortie VPC géré par le client pour acheminer le trafic sortant via votre VPC à la place.

Un seul connecteur peut être réutilisé sur de nombreuses microVM. C'est le modèle d'utilisation prévu.

Connectivité entrante

Chaque microVM Lambda est accessible via une URL de point de terminaison HTTPS unique, attribuée lorsque vous appelez. `run-microvm` Les clients envoient des demandes à ce point de terminaison via HTTPS. Lambda achemine chaque demande vers un port de votre microVM, où votre application la reçoit.

Par défaut, les demandes reçues sur le point de terminaison sont acheminées vers le port 8080 à l'intérieur de la microVM. Pour effectuer un routage vers un autre port, voirthe section called “Routage des ports”.

Les protocoles suivants sont pris en charge sur le point de terminaison entrant :

- HTTP/1.1
- HTTP/2

- WebSockets
- gRPC
- Server-Sent Événements (SSE)

> **Note**
>
> Le trafic entre votre client et le point de terminaison microVM est toujours chiffré avec le protocole TLS. Votre application peut traiter des requêtes via HTTP ou HTTPS en interne.

Routage des ports

Lambda sélectionne le port cible dans votre microVM selon l'ordre de priorité suivant :

1. **`X-aws-proxy-port`**en-tête — Pour les requêtes HTTP standard, incluez cet en-tête avec le numéro de port cible.
2. WebSocket sous-protocole — Si votre WebSocket client ne parvient pas à définir des en-têtes personnalisés, spécifiez le port cible sous forme de sous-protocole nommé`lambda-microvms.port.`*`N`*, où *`N`* est le numéro de port. Vous fournissez des sous-protocoles lorsque vous ouvrez la WebSocket connexion. Pour obtenir un exemple, consultez the section called “Protocoles”.
3. Par défaut (8080) — Si aucun des deux n'est spécifié, demande la route vers le port 8080.

> **Important**
>
> Le port cible doit être compris dans les limites `allowedPorts` définies dans le jeton d'authentification. Les demandes adressées à des ports non autorisés reçoivent une réponse 403 Forbidden.

Authentification

Toutes les demandes adressées à un point de terminaison microVM nécessitent un jeton d'authentification valide dans l'`X-aws-proxy-auth`en-tête. Vous générez des jetons en utilisant`create-microvm-auth-token`. Chaque jeton est une chaîne JWE (JSON Web Encryption) cryptée dont la portée est la suivante :

- Une microVM spécifique (identifiée par un ID).
- Un ensemble de ports autorisés (port unique, plage ou tous les ports).
- Un délai d'expiration (configuré lors de la création du jeton).

L'exemple suivant crée un jeton et l'utilise pour envoyer une demande authentifiée :

```
aws lambda-microvms create-microvm-auth-token \
  --microvm-identifier microvm-id \
  --expiration-in-minutes 30 \
  --allowed-ports '[{"port":8080}]'
```

```
curl 'https://microvm-endpoint' \
  -H 'X-aws-proxy-auth: TOKEN' \
  -H 'X-aws-proxy-port: 8080'
```

Pour une présentation complète de la création de jetons et de la connexion à une microVM, y compris WebSocket les connexions, voir. the section called “Connexion à une microVM”

Réponses d’erreur

Les codes d'état HTTP suivants sont renvoyés par le point de terminaison microVM lorsqu'il ne peut pas traiter ou envoyer une demande à votre application. Ces réponses proviennent du point de terminaison, et non de votre application.

Code	Statut	Cause et résolution
400	Demande erronée	Demande mal formée, en-tête de port ou WebSocket sous-protocole non valide. Vérifiez le format.
403	Accès interdit	Jeton manquant, expiré ou non valide ; ou le port demandé ne figure pas dans celui du jeton`allowedPorts` . Générez un nouveau jeton ou utilisez un port autorisé.
429	Nombre de demandes trop élevé	Limite de débit dépassée (au niveau du compte ou par microVM). Réessayez avec un recul exponentiel.

Code	Statut	Cause et résolution
500	Erreur de serveur interne	Une erreur interne s'est produite. Réitérez la demande.
502	Passerelle erronée	L'application ne répond pas ou la reprise automatique n'a pas réussi dans le nombre maximal de tentatives. Consultez the section called "Auto-resume".

En-têtes de demandes

L'espace de noms `X-aws-proxy-*` d'en-tête est réservé par Lambda aux métadonnées de demande, telles que le jeton d'authentification `X-aws-proxy-auth` () et le port `X-aws-proxy-port` cible (). Lambda supprime les `X-aws-proxy-*` en-têtes avant de transmettre la demande à votre application.

Request/response bande passante

Chaque microVM Lambda dispose d'une request/response bande passante qui s'adapte linéairement à sa taille. Cette bande passante s'applique à tout le trafic passant par le point de terminaison MicroVM, à la fois aux demandes entrantes et aux réponses sortantes.

Taille de la microVM (référence)	Bande passante maximale
0,5 GO, 0,25 vCPU	1 MB/s (8 Mbits/s)
1 GO, 0,5 vCPU	2 MB/s (16 Mbits/s)
2 GO, 1 vCPU	4 MB/s (32 Mbits/s)
4 GO, 2 vCPU	8 MB/s (64 Mbits/s)
8 GO, 4 vCPU	16 MB/s (128 Mbits/s)

Si la latence des demandes augmente en raison de la saturation du réseau, réduisez la simultanéité de vos demandes ou la taille de la charge utile, ou sélectionnez une taille de microVM plus grande pour augmenter la bande passante disponible.

HTTP/2 soutien

Lambda MicroVMS prend en charge HTTP/2 le point de terminaison entrant. Lambda négocie le protocole via ALPN (Application-Layer Protocol Negotiation) lors de la poignée de main TLS, en privilégiant et en revenant à. HTTP/2 HTTP/1.1 Un HTTP/2-capable client l'utilise automatiquement.

À utiliser HTTP/2 entre le point de terminaison et votre application dans le microVM :

- Votre application utilise le protocole TLS : Lambda HTTP/2 négocie avec votre application via ALPN, puis revient à la solution si elle n'est pas prise HTTP/1.1 en HTTP/2 charge.
- Votre application sert du HTTP en texte brut : incluez l'`X-aws-proxy-force-h2: true`en-tête dans votre demande à utiliser HTTP/2 lors de la connexion à votre application.

Connectivité sortante

Par défaut, les microVM Lambda disposent d'un accès Internet public sur le chemin de sortie. Pour connecter des microVM aux ressources de vos VPC privés, telles que le RDS ElastiCache, les API internes et les systèmes sur site via Direct Connect ou VPN, créez un connecteur réseau Lambda avec votre configuration VPC.

Lorsque vous utilisez la sortie VPC, le trafic sortant est soumis aux règles des groupes de sécurité et aux ACL du réseau qui régissent le trafic dans votre VPC.

Utilisation de connecteurs réseau de sortie

Les connecteurs réseau de sortie acheminent le trafic sortant de votre microVM via votre VPC. Vous créez un connecteur une fois, puis vous le référencez par ARN lors du démarrage de MicroVMS via la `run-microvm` commande.

Conditions préalables

Avant de créer un connecteur réseau, vous avez besoin d'un rôle IAM qui permet à Lambda de créer des interfaces réseau élastiques (ENI) dans votre VPC. Ce rôle requiert les autorisations suivantes :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CreateENI",
```

```
      "Effect": "Allow",
      "Action": "ec2:CreateNetworkInterface",
      "Resource": [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid": "TagENI",
      "Effect": "Allow",
      "Action": "ec2:CreateTags",
      "Resource": "arn:aws:ec2:*:*:network-interface/*",
      "Condition": {
        "StringEquals": {
          "ec2:ManagedResourceOperator": "network-connectors.lambda.amazonaws.com"
        }
      }
    }
  ]
}
```

Création d'un connecteur réseau

Créez un connecteur en spécifiant vos sous-réseaux VPC, vos groupes de sécurité et votre protocole réseau (`IPv4`ou) : `DualStack`

```
aws lambda-core create-network-connector \
  --name my-connector \
  --configuration '{
    "VpcEgressConfiguration": {
      "SubnetIds": ["subnet-xxx"],
      "SecurityGroupIds": ["sg-xxx"],
      "NetworkProtocol": "IPv4",
      "AssociatedComputeResourceTypes": ["MicroVm"]
    }
  }' \
  --operator-role arn:aws:iam::123456789012:role/NetworkConnectorOperatorRole
```

États du connecteur réseau

Un connecteur doit être en `ACTIVE` état pour que vous puissiez le référencer`run-microvm`.

State	Description
PENDING	Le connecteur est en cours de création (les ENI sous-jacents sont en cours de provisionnement).
ACTIVE	Le connecteur est prêt à être utilisé.
INACTIVE	Le connecteur est temporairement inactif.
FAILED	Le provisionnement ou la mise à jour ont échoué. Vérifiez StateReason .
DELETING	Le connecteur est en cours de suppression ; les ENI sont en cours de nettoyage.
DELETE_FAILED	La suppression a échoué.

Gestion des versions des connecteurs réseau

Le versionnement s'applique aux connecteurs réseau de sortie VPC (type de connecteur). VPC_EGRESS Un connecteur de sortie VPC est versionné : chaque update-network-connector appel réussi crée une nouvelle version, et les versions antérieures restent disponibles.

Lorsque vous exécutez une microVM, vous référencez un connecteur de sortie VPC par ARN in. --egress-network-connectors Vous pouvez utiliser l'un ou l'autre des formulaires suivants :

- ARN non qualifié : correspond à la dernière version du connecteur. Une microVM enregistre automatiquement les modifications de configuration. arn:aws:lambda:*us-east-1*:*123456789012*:network-connector:*nc-id*
- ARN qualifié : associe le microVM à une version spécifique. Utilisez-le pour maintenir une microVM sur une configuration connue à des fins de test, de dépannage ou de restauration. arn:aws:lambda:*us-east-1*:*123456789012*:network-connector:*nc-id*:*version-number*

Une microVM passe à une nouvelle version uniquement lorsque vous modifiez l'ARN auquel elle fait référence, afin que vous puissiez adopter de nouvelles versions selon votre propre calendrier.

Exemple run-microvm d'appel visant à épingler une version de connecteur spécifique :

```
aws lambda-microvms run-microvm \
  --image-identifier arn:aws:lambda:us-east-1:123456789012:microvm-image:my-microvm-image \
  --egress-network-connectors arn:aws:lambda:us-east-1:123456789012:network-connector:nc-id:version-number \
  --idle-policy
 '{"maxIdleDurationSeconds":900,"suspendedDurationSeconds":1800,"autoResumeEnabled":false}'
```

Exécution d'une microVM avec un connecteur réseau

Référencez l'ARN du connecteur lors de l'exécution d'une microVM :

```
aws lambda-microvms run-microvm \
  --image-identifier arn:aws:lambda:us-east-1:123456789012:microvm-image:my-microvm-image \
  --egress-network-connectors connector-arn \
  --idle-policy
 '{"maxIdleDurationSeconds":900,"suspendedDurationSeconds":1800,"autoResumeEnabled":false}'
```

> **Note**
>
> Avant de mettre à jour ou de supprimer un connecteur, assurez-vous que toutes les microVM qui l'utilisent sont hors service. La modification d'un connecteur activement utilisé peut entraîner des problèmes de connectivité réseau lors de l'exécution de microVM.

Utilisation de microVM Lambda avec des points de terminaison VPC d'interface (AWS PrivateLink)

Vous pouvez utiliser AWS PrivateLink une connectivité privée sur le AWS réseau entre vos ressources VPC et les microVM Lambda, sans passer par l'Internet public. MicroVMS prend en charge deux points de terminaison VPC, en fonction de la destination du trafic souhaitée :

- API de gestion MicroVM (création d'images, exécution, suspension, arrêt) : utilisent le point de terminaison `com.amazonaws.region.lambda` VPC Lambda existant ().
- Connectivité aux microVM (trafic HTTPS vers vos applications en cours d'exécution) : utilise un point de terminaison distinct (`com.amazonaws.region.lambda-microvm`).

Point de terminaison VPC pour les API de gestion de microVM

Lambda MicroVMS partage le même service de point de terminaison VPC que Lambda (). `com.amazonaws.region.lambda` Pour obtenir des instructions complètes, consultez Création d'un point de terminaison d'interface pour Lambda.

Politique de point de terminaison pour les API de gestion des micromachines virtuelles

Pour contrôler qui peut utiliser le point de terminaison de votre interface et quelles actions d'API Lambda microVMS ils peuvent effectuer, associez une politique de point de terminaison. La politique indique le principal habilité à effectuer des actions, les actions qu'il peut effectuer et les ressources sur lesquelles il peut agir. Les actions Lambda MicroVMS utilisent le préfixe d'action IAM. `lambda:`

Pour plus d'informations, consultez Contrôle de l'accès aux services avec points de terminaison d'un VPC dans le Guide de l'utilisateur Amazon VPC.

L'exemple de politique suivant permet `MyUser` à l'utilisateur de répertorier et d'obtenir des images microVM via le point de terminaison :

```
{
  "Statement": [
    {
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:user/MyUser"
      },
      "Effect": "Allow",
      "Action": [
        "lambda:ListMicrovmImages",
        "lambda:GetMicrovmImage"
      ],
      "Resource": "*"
    }
  ]
}
```

Point de terminaison VPC pour la connectivité microVM

Pour que le trafic HTTPS vers vos microVM en cours d'exécution reste privé, créez un point de terminaison d'interface pour le `com.amazonaws.region.lambda-microvm` service. Ce point de terminaison gère les connexions aux URL des points de terminaison microVM (par exemple,`abc123def456.lambda-microvm.us-east-1.on.aws`).

Pour en savoir plus sur les propriétés des points de terminaison d'interface, consultez le guide des points de terminaison d'interface dans la documentation Amazon VPC.

Création du point de terminaison

Pour créer un point de terminaison d'interface pour la connectivité microVM (console)

1. Ouvrez la page Points de terminaison de la console Amazon VPC.
2. Choisissez Créer un point de terminaison.
3. Pour Catégorie de service, assurez-vous que Services AWS est sélectionné.
4. Pour Service Name (Nom du service), choisissez `com.amazonaws.region.lambda-microvm`. Vérifiez que le type est Interface.
5. Choisissez un VPC et des sous-réseaux
6. Pour activer le DNS privé pour le point de terminaison de l'interface, cochez la case Activer le nom DNS (recommandé). Cela garantit que les demandes utilisant le nom d'hôte public du point de terminaison microVM sont automatiquement résolues vers le point de terminaison de votre interface, sans qu'aucune modification côté client ne soit requise.
7. Pour Groupes de sécurité, choisissez un ou plusieurs groupes de sécurité. Le groupe de sécurité doit autoriser le trafic TCP sortant sur le port 443 vers les interfaces réseau des terminaux.
8. Choisissez Créer un point de terminaison.

Pour utiliser l'option DNS privé, vous devez définir les `enableDnsSupport` attributs `enableDnsHostnames` et de votre VPC. Pour plus d'informations, consultez Affichage et mise à jour de la prise en charge de DNS pour votre VPC dans le Guide de l'utilisateur Amazon VPC.

Pour créer un point de terminaison d'interface pour la connectivité microVM (AWS CLI)

```
aws ec2 create-vpc-endpoint \
  --vpc-id vpc-ec43eb89 \
  --vpc-endpoint-type Interface \
  --service-name com.amazonaws.us-east-1.lambda-microvm \
  --subnet-id subnet-abababab \
  --security-group-id sg-1a2b3c4d \
  --private-dns-enabled
```

Pour vérifier que le point de terminaison est disponible et que le DNS privé est activé :

```
aws ec2 describe-vpc-endpoints \
```

```
  --vpc-endpoint-ids vpce-1a2b3c4d5e6f7g8h9 \
  --query 'VpcEndpoints[0].
{State:State,PrivateDns:PrivateDnsEnabled,Dns:DnsEntries[*].DnsName}'
```

Comportement du DNS privé

Lorsque le DNS privé est activé : le point de terminaison gère la résolution DNS pour `*.lambda-microvm.region.on.aws` l'intérieur de votre VPC. Les noms d'hôte de vos points de terminaison MicroVM existants (par exemple,`abc123def456.lambda-microvm.us-east-1.on.aws`) sont les adresses IP privées des interfaces réseau des points de terminaison. Aucun changement de client n'est requis.

Lorsque le DNS privé est désactivé, Amazon VPC génère un nom DNS spécifique au point de terminaison pour votre point de terminaison dans le formulaire. `vpce-id-hash.lambda-microvm.region.vpce.amazonaws.com` Pour acheminer le trafic via ce point de terminaison tout en atteignant le microVM approprié, vous devez conserver le nom d'hôte microVM d'origine à deux endroits :

- Indication du nom du serveur TLS (SNI) : le handshake TLS utilise cette valeur pour identifier la microVM à laquelle la connexion est destinée.
- En-tête HTTP Host — Le proxy utilise cette valeur pour acheminer la demande vers le microVM approprié.

Si l'une des valeurs est définie sur le nom d'hôte du point de terminaison VPC au lieu du nom d'hôte de la microVM, la connexion ne peut pas être routée vers la microVM appropriée.

Exemple : Connexion via un nom DNS spécifique au point de terminaison

L'exemple suivant utilise curl avec l'`--connect-to`indicateur pour rediriger la connexion TCP vers votre point de terminaison VPC tout en conservant le nom d'hôte microVM dans l'URL, le SNI et l'en-tête Host :

```
ENDPOINT_HOST=abc123def456.lambda-microvm.us-east-1.on.aws
VPCE_HOST=vpce-0a1b2c3d4e5f67890-a1b2c3d4.lambda-microvm.us-east-1.vpce.amazonaws.com

curl --connect-to "$ENDPOINT_HOST:443:$VPCE_HOST:443" \
  -H "x-aws-proxy-auth: $MICROVM_AUTH_TOKEN" \
  -H "x-aws-proxy-port: 8080" \
  "https://$ENDPOINT_HOST/"
```

L'`--connect-to`indicateur indique à curl d'ouvrir la connexion TCP à l'adresse du point de terminaison VPC, tandis que l'URL, le TLS SNI et l'en-tête Host restent définis sur le nom d'hôte de votre microVM.

Pour plus d'informations, consultez Accès à un service via un point de terminaison d'interface dans le Guide de l'utilisateur Amazon VPC.

Politique de point de terminaison pour la connectivité des micromachines virtuelles

Vous pouvez associer une politique de point de terminaison pour contrôler les microVM accessibles via le point de terminaison VPC. `lambda-microvm` Une politique de point de terminaison sur le `lambda-microvm` service vous permet de définir les connexions à des comptes ou à des organisations spécifiques. Par défaut, le point de terminaison autorise les connexions aux microVM depuis n'importe quel AWS compte. (Remarque : le client établissant la connexion doit toujours détenir un jeton d'authentification MicroVM valide pour pouvoir y accéder).

Par défaut, un point de terminaison VPC dispose d'une politique d'accès complet qui autorise tout le trafic. Lorsque vous remplacez la politique par défaut par une politique personnalisée, Lambda microVMS évalue cette politique par rapport à l'`lambda:ConnectMicrovm`action sur chaque connexion établie via le point de terminaison. Si la politique n'autorise pas la connexion aux microVM, la connexion est rejetée avec une réponse HTTP 403 Forbidden. Une politique qui n'accorde pas d'autorisation `lambda:ConnectMicrovm` refuse toutes les connexions via le point de terminaison.

> **Note**
>
> L'`lambda:ConnectMicrovm`action autorise une connexion à un point de terminaison microVM via le point de terminaison de l'interface. Il ne s'agit pas d'une opération d'API Lambda et ne peut pas être utilisée dans les politiques IAM basées sur l'identité ou les ressources. Elle n'est valide que dans une politique de point de terminaison VPC.

Principal et ressource

Les connexions à un point de terminaison microVM sont authentifiées à l'aide d'un jeton d'authentification microVM plutôt que AWS de Signature version 4. Pour cette raison, aucun principal IAM n'est associé à la connexion. Lambda MicroVMS évalue plutôt la politique du point de terminaison avec un principal anonyme. Autrement dit :

- `Principal` doit avoir pour valeur `"*"`. Une politique qui nomme un principal spécifique ne correspond à rien et refuse toute connexion.

- Les clés de condition qui dépendent de l'identité du demandeur (telles que `aws:PrincipalArn`aws:PrincipalOrgID, et`aws:userid`) ne sont pas renseignées et ne correspondent pas.
- `Resource`doit également l'être`"*"`. Lambda MicroVMS n'étend pas l'évaluation des politiques de point de terminaison aux ARN de ressources microVM individuels. Pour limiter les microVM que le point de terminaison peut atteindre, utilisez la clé de `aws:ResourceAccount` condition plutôt que l'`Resource`élément.

Clés de condition prises en charge

Clé de condition	Description
`aws:ResourceAccount`	Le AWS compte propriétaire de la microVM à laquelle vous êtes connecté.
`aws:ResourceOrgID`	L'ID d'organisation AWS Organizations du compte propriétaire de la microVM.
`aws:SourceVpce`	ID du point de terminaison de l'interface par lequel la connexion est passée.
`aws:SourceVpc`	L'ID du VPC d'où provient la connexion.
`aws:VpcSourceIp`	Adresse IP privée du client qui a établi la connexion.

Exemple : autoriser les connexions uniquement aux microVM dans votre propre compte

La politique de point de terminaison suivante autorise les connexions via le point de terminaison uniquement aux microVM détenues par le compte 111122223333. Les connexions aux microVM appartenant à un autre compte sont refusées.

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": "lambda:ConnectMicrovm",
      "Resource": "*",
```

```
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "111122223333"
        }
      }
    }
  ]
}
```

Sécurité et autorisations

Cette section décrit les rôles IAM, les jetons d'authentification et les contrôles d'accès pour les AWS Lambda micromachines virtuelles.

Rôles IAM

Créer un rôle

Ce rôle est utilisé lors de la création de l'image. Les autorisations suivantes sont requises pour récupérer les artefacts sources et générer des journaux : `s3:GetObject`logs:CreateLogGroup,`logs:CreateLogStream`, et`logs:PutLogEvents`. Ajoutez également `ecr:GetAuthorizationToken` si vous faites référence à des images ECR privées.

Le rôle de génération est facultatif. Si vous ne fournissez pas de rôle de génération, Lambda ne peut pas écrire de journaux de génération dans CloudWatch.

Rôle d'exécution

Ce rôle est utilisé lors de l'exécution de MicroVM pour fournir des autorisations d'accès permettant d'écrire des journaux CloudWatch et d'utiliser d'autres AWS services.

Le rôle d'exécution est facultatif. Si vous ne fournissez pas de rôle d'exécution, Lambda n'émet pas de journaux d'exécution vers d'autres services CloudWatch et votre microVM ne peut pas accéder à d'autres AWS services.

Les hooks Lifecycle s'exécutent sous le rôle associé à leur phase. Build-time hooks (`/readyet/validate`) s'exécutent sous le rôle build. Les hooks d'exécution (`/run/resume`,`/suspend`, et`/terminate`) s'exécutent sous le rôle d'exécution.

Politiques d’approbation

Les deux rôles nécessitent une politique de confiance qui permet au principal du service Lambda `lambda.amazonaws.com` d'exécuter `sts:AssumeRole` et`sts:TagSession`.

Jetons d'authentification

Les jetons contrôlent l'accès entrant aux micromachines virtuelles en cours d'exécution. Ils sont délimités par port ; chaque jeton spécifie les ports auxquels il autorise l'accès.

```
# Token granting access to all ports
aws lambda-microvms create-microvm-auth-token \
  --microvm-identifier <id> \
  --expiration-in-minutes 30 \
  --allowed-ports '[{"allPorts":{}}]'

# Token granting access to port 8080 only
aws lambda-microvms create-microvm-auth-token \
  --microvm-identifier <id> \
  --expiration-in-minutes 30 \
  --allowed-ports '[{"port":8080}]'
```

Jetons d'accès Shell

L'accès au shell utilise une API de jeton distincte. La microVM cible doit avoir été exécutée avec le connecteur `SHELL_INGRESS` réseau (`arn:aws:lambda:us-east-1:aws:network-connector:aws-network-connector:SHELL_INGRESS`). Si la microVM n'a pas été lancée avec ce connecteur, elle `create-microvm-shell-auth-token` échoue avec le message suivant : `ValidationException`

```
aws lambda-microvms create-microvm-shell-auth-token \
  --microvm-identifier <id> \
  --expiration-in-minutes 30
```

Pour une présentation complète de la connexion à un shell MicroVM, consultez. the section called “Accès au shell”

Balisage de ressources

Les images Lambda MicroVM prennent en charge les balises de AWS ressources pour l'organisation et la répartition des coûts. Ajoutez des balises lors de la création d'une image à l'aide du `--tags`

paramètre ou explicitement après la création. Vous pouvez également répertorier et supprimer des balises, comme illustré ci-dessous : Vous pouvez également faire référence à des balises dans les conditions de politique IAM afin de contrôler l'accès aux ressources microVM.

```
# Add tags when creating an image
aws lambda-microvms create-microvm-image \
  --name my-app-image \
  --code-artifact '{"uri":"s3://my-bucket/app.zip"}' \
  --base-image-arn arn:aws:lambda:us-east-1:aws:microvm-image:al2023-1 \
  --build-role-arn arn:aws:iam::123456789012:role/MicrovmBuildRole \
  --tags '{"Environment":"production","Team":"platform"}'

# List tags on a resource
aws lambda-microvms list-tags \
  --resource arn:aws:lambda:us-east-1:123456789012:microvm-image:my-app-image

# Add tags to an existing resource
aws lambda-microvms tag-resource \
  --resource arn:aws:lambda:us-east-1:123456789012:microvm-image:my-app-image \
  --tags '{"CostCenter":"12345","Project":"sandbox-platform"}'

# Remove tags by key
aws lambda-microvms untag-resource \
  --resource arn:aws:lambda:us-east-1:123456789012:microvm-image:my-app-image \
  --tag-keys '["CostCenter","Project"]'
```

Référence des autorisations IAM

Lambda MicroVMS définit les actions IAM suivantes. Utilisez-les dans les politiques IAM pour contrôler l'accès aux opérations de microVM.

Action	Description
`lambda:CreateMicrovmImage`	Créez une nouvelle image MicroVM.
`lambda:UpdateMicrovmImage`	Mettez à jour une image microVM existante.
`lambda:DeleteMicrovmImage`	Supprimez une image MicroVM.
`lambda:GetMicrovmImage`	Obtenez les détails de l'image MicroVM.

Action	Description
`lambda:ListMicrovmImages`	Répertoriez les images MicroVM du compte.
`lambda:RunMicrovm`	Exécutez une nouvelle microVM.
`lambda:GetMicrovm`	Obtenez l'état et les détails de la microVM.
`lambda:ListMicrovms`	Répertoriez les micromachines virtuelles du compte.
`lambda:SuspendMicrovm`	Suspendez une microVM en cours d'exécution.
`lambda:ResumeMicrovm`	Reprenez une microVM suspendue.
`lambda:TerminateMicrovm`	Mettez fin à une microVM.
`lambda:CreateMicrovmAuthToken`	Générez un jeton d'authentification pour une microVM.
`lambda:CreateMicrovmShellAuthToken`	Générez un jeton d'accès au shell.

Formats ARN des ressources

```
# MicroVM image
arn:aws:lambda:<region>:<account>:microvm-image:<image-name>
# Network connector
arn:aws:lambda:<region>:<account>:network-connector:<connector-id>
```

Exemple : Least-privilege politique pour un opérateur

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
          "lambda:ListMicrovms",
          "lambda:ListMicrovmImages"
        ],
```

```
        "Resource": "*"
      },
      {
        "Effect": "Allow",
        "Action": [
          "lambda:RunMicrovm",
          "lambda:GetMicrovm",
          "lambda:SuspendMicrovm",
          "lambda:ResumeMicrovm",
          "lambda:TerminateMicrovm",
          "lambda:CreateMicrovmAuthToken",
          "lambda:GetMicrovmImage"
        ],
        "Resource": "arn:aws:lambda:*:123456789012:microvm-image:*"
      }
    ]
}
```

Contrôle

Cette page couvre la CloudWatch journalisation (génération et exécution) et l' CloudTrail audit pour les AWS Lambda micromachines virtuelles.

Journalisation (CloudWatch journaux)

AWS Lambda MicroVMS diffuse les logs vers lesquels elle transmet les logs CloudWatch en deux phases :

Créez des journaux

Lambda génère des journaux de génération lors de la création de l'image, y compris les résultats de `Dockerfile` l'exécution, du démarrage de l'application et des invocations de hooks. Ces journaux sont diffusés à l'aide du rôle de génération et écrits dans le groupe `/aws/lambda-microvms/<image-name>` de journaux par défaut.

Journaux d'exécution

Lambda diffuse les applications stdout et stderr depuis l'exécution de MicroVMS vers. CloudWatch Les journaux d'exécution sont transmis en continu à l'aide du rôle d'exécution et écrits dans le même groupe de journaux par défaut, le flux de journaux utilisant par défaut l'ID microVM.

> **Important**
>
> Sans rôle d'exécution, les applications stdout et stderr ne sont pas transmises au moment de l'exécution. CloudWatch Pour recevoir les journaux d'exécution, indiquez un rôle d'exécution avec `logs:CreateLogGrouplogs:CreateLogStream`, et `logs:PutLogEvents` des autorisations.

Destinations de journaux personnalisées

Vous pouvez configurer un groupe de journaux et un flux personnalisés à l'aide du `--logging` paramètre on `run-microvm` ou `create-microvm-image` :

```
--logging '{"cloudWatch":{"logGroup":"/my-app/microvms","logStream":"custom-stream"}}'
```

Si vous l'omettez`logStream`, la valeur par défaut est l'ID de la microVM.

Vous pouvez désactiver explicitement la journalisation en passant la configuration suivante :

```
--logging '{"disabled":{}}'
```

CloudTrail journalisation

Lambda MicroVM est intégrée à CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service. CloudTrail capture tous les appels d'API pour les microVM Lambda sous forme d'événements. Les appels capturés incluent les appels depuis la console Lambda MicroVMS et les appels de code vers les opérations de l'API Lambda MicroVMS.

Si vous créez un historique, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris des événements pour Lambda MicroVMS. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents sur la CloudTrail console dans l'historique des événements.

À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite à Lambda MicroVMS, l'adresse IP à partir de laquelle la demande a été faite, qui a effectué la demande, quand elle a été faite et des informations supplémentaires.

CloudTrail enregistre deux types d'événements pour les micromachines virtuelles Lambda : les événements de gestion (opérations du plan de contrôle telles que la création et la suppression

d'images) et les événements liés aux données (opérations du plan de données telles que l'exécution et la fin de micromachines virtuelles). Les événements de gestion sont enregistrés par défaut. Les événements liés aux données nécessitent une inscription explicite.

Événements de gestion

Les événements de gestion Lambda MicroVMS sont des opérations du plan de contrôle qui sont enregistrées par défaut. CloudTrail Les événements de gestion incluent la création, la mise à jour et la suppression d'images MicroVM, ainsi que la liste et la description des ressources.

Les actions Lambda MicroVMS suivantes sont enregistrées en tant qu'événements de gestion :

- `CreateMicrovmImage`
- `DeleteMicrovmImage`
- `DeleteMicrovmImageVersion`
- `UpdateMicrovmImage`
- `UpdateMicrovmImageVersion`
- `ListMicrovmImages`
- `GetMicrovmImage`
- `ListMicrovmImageVersions`
- `GetMicrovmImageVersion`
- `ListMicrovmImageBuilds`
- `GetMicrovmImageBuild`
- `ListMicrovms`
- `GetMicrovm`
- `ListManagedMicrovmImages`

Événements de données

Les événements de données fournissent des informations sur les opérations de ressources effectuées sur ou au sein d'une ressource (par exemple, l'exécution ou l'arrêt d'une microVM). Ils sont également connus sous le nom opérations de plans de données. Les événements de données sont souvent des activités à fort volume. Par défaut, CloudTrail n'enregistre pas les événements liés aux données. Vous devez activer explicitement la journalisation des événements de données pour Lambda MicroVMS.

Le type de CloudTrail ressource pour les événements de données Lambda MicroVMS est. `AWS::Lambda::MicrovmImage` Vous pouvez utiliser la CloudTrail console ou l' AWS interface de ligne de commande pour configurer un journal ou un magasin de données d'événements afin de consigner les événements de données.

Les actions Lambda MicroVMS suivantes sont enregistrées en tant qu'événements de données :

- `RunMicrovm`
- `TerminateMicrovm`
- `SuspendMicrovm`
- `ResumeMicrovm`
- `CreateMicrovmAuthToken`
- `CreateMicrovmShellAuthToken`

Pour enregistrer les événements de données pour toutes les images MicroVM, utilisez le sélecteur d'événements avancé suivant :

```
{
   "Name": "Log Lambda MicroVM data events",
   "FieldSelectors": [
     { "Field": "eventCategory", "Equals": ["Data"] },
     { "Field": "resources.type", "Equals": ["AWS::Lambda::MicrovmImage"] }
   ]
}
```

Activation de l'enregistrement des événements de données

Pour activer la journalisation des événements de données à l'aide de l' AWS interface de ligne de commande, exécutez la `put-event-selectors` commande à l'aide de sélecteurs d'événements avancés :

```
aws cloudtrail put-event-selectors \
   --trail-name my-trail \
   --advanced-event-selectors '[{
     "Name": "Log Lambda MicroVM data events",
     "FieldSelectors": [
       { "Field": "eventCategory", "Equals": ["Data"] },
       { "Field": "resources.type", "Equals": ["AWS::Lambda::MicrovmImage"] }
```

```
    ]
  }]'
```

Comprendre les entrées de CloudTrail journal

Un journal CloudTrail transmet les enregistrements d'activité de l'API à un compartiment Amazon S3 que vous spécifiez. Chaque entrée de journal représente une seule demande d'API et inclut l'identité de l'appelant, l'horodatage, les paramètres de demande et la réponse.

L'exemple suivant montre une entrée de CloudTrail journal qui illustre un événement de données pour l'`RunMicrovm`action :

```
{
  "eventVersion": "1.11",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "A1B2C3D4E5F6G7EXAMPLE:mySessionName",
    "arn": "arn:aws:sts::111122223333:assumed-role/MyRole/mySessionName",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE"
  },
  "eventTime": "2026-04-20T18:26:44Z",
  "eventSource": "lambda.amazonaws.com",
  "eventName": "RunMicrovm",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "127.0.0.1",
  "requestParameters": {
    "microvmImageArn": "arn:aws:lambda:us-east-1:111122223333:microvm-image:my-image"
  },
  "responseElements": {
    "microvmId": "ai-12345678-abcd-1234-ef56-123456789abc",
    "microvmState": "PENDING",
    "endpoint": "12345678-abcd-1234-ef56-123456789abc.lambda-microvm.us-east-1.on.aws",
    "microvmImageArn": "arn:aws:lambda:us-east-1:111122223333:microvm-image:my-image",
    "microvmImageVersion": "1.0"
  },
  "requestID": "7aebcd0f-cda1-11e4-aaa2-e356da31e4ff",
  "eventID": "e92a3e85-8ecd-4d23-8074-843aabfe89bf",
  "readOnly": false,
  "resources": [
    {
      "accountId": "111122223333",
      "type": "AWS::Lambda::MicrovmImage",
```

```
      "ARN": "arn:aws:lambda:us-east-1:111122223333:microvm-image:my-image"
    }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": false,
  "recipientAccountId": "111122223333",
  "eventCategory": "Data"
}
```

Résolution des problèmes

Cette section décrit comment déboguer et résoudre les problèmes courants liés à l'utilisation de MicroVMS. AWS Lambda

Accès au shell

Utilisez l'accès au shell pour vous connecter directement à une microVM en cours d'exécution à des fins de débogage et de dépannage.

Vous pouvez vous connecter à un shell MicroVM de deux manières :

- Console : sélectionnez votre microVM dans la console Lambda et choisissez Connect.
- CLI : générez un jeton shell avec`create-microvm-shell-auth-token`, puis utilisez-le pour établir une connexion.

Générez un jeton shell, puis connectez-vous :

```
aws lambda-microvms create-microvm-shell-auth-token \
  --microvm-identifier <id> --expiration-in-minutes 30
# In Console: select MicroVM -> Connect
# In shell: ctr task ls, then ctr task exec -t --exec-id shell <id> /bin/sh
```

La microVM doit avoir été exécutée avec le connecteur `SHELL_INGRESS` réseau (`arn:aws:lambda:`*`us-east-1`*`:aws:network-connector:aws-network-connector:SHELL_INGRESS`). Si la microVM n'a pas été lancée avec ce connecteur, `create-microvm-shell-auth-token` renvoie un`ValidationException`.

Pour les autres questions :

- Vérifiez le `terminationMessage` champ de la `get-microvm` réponse pour les micromachines virtuelles résiliées.
- Consultez les journaux CloudWatch de génération pour détecter les problèmes liés à la création d'images.
- Vérifiez le `StateReason` champ correspondant aux connecteurs réseau en `FAILED` état.

Résolution des problèmes

Cette section propose des solutions aux problèmes courants liés à l'utilisation de Lambda MicroVMS.

Symptôme	Cause possible et résolution
La génération de l'image échoue (`CREATION_FAILED`)	Consultez les journaux de construction à l'adresse `/aws/lambda-microvms/<image-name>`. Vérifiez `Dockerfile` la syntaxe, les autorisations Amazon S3 et la disponibilité des images de base. Exécutez `docker build` localement pour reproduire.
MicroVM bloquée `PENDING`	Patientez et réessayez. En cas de persistance, vérifiez l'état du service. Vérifiez que votre quota de simultanéité n'est pas épuisé.
La candidature ne répond pas après le CV	Implémentez le hook `/resume` du cycle de vie pour rétablir les connexions et valider l'état. Vérifiez que votre application est liée au port 8080 (ou au port configuré) après la reprise.
502 Passerelle défectueuse depuis le terminal	L'application s'est bloquée ou n'écoute pas. Vérifiez les journaux d'exécution. Vérifiez `EXPOSE` et `CMD` entrez`Dockerfile`. En cas de reprise automatique, la microVM n'a peut-être pas pu reprendre (vérifiez l'état à l'aide `get-microvm` de).
429 demandes de trop	Taux de demandes dépassé. Réessayez avec un ralentissement exponentiel et de la gigue.
Suppression des connexions	Délai d'inactivité déclenché. Mettez en œuvre des ping/pong keepalives. Ou prolongez `maxIdleDurationSeconds` la politique d'inactivité.

Symptôme	Cause possible et résolution
Latence élevée sur le terminal	Saturation de la bande passante. Vérifiez si le trafic dépasse la capacité de bande passante correspondant à la taille de votre microVM. Passez à une taille plus grande.
Le jeton d'authentification a expiré (403)	Les jetons ont une date d'expiration configurable. Générez un nouveau jeton avant que l'ancien n'expire. Implémentez une logique d'actualisation des jetons dans votre client.
La sortie du VPC ne fonctionn e pas	Vérifiez que le connecteur réseau est en `ACTIVE` état. Vérifiez que les règles des groupes de sécurité autorisent le trafic sortant. Vérifiez que les sous-réseaux disposent d'itinéraires vers vos ressources cibles.

Erreurs courantes (création d'images)

Erreur	Cause	Solution
`S3_ACCESS_DENIED`	Le rôle de compilation n'est pas autorisé à récupérer l'artefact Amazon S3.	Ajoutez une `s3:GetObj ect` autorisation pour votre compartiment d'artefacts.
`S3_NO_SUCH_KEY`	La clé d'artefact n'existe pas dans le compartiment.	Vérifiez que le chemin Amazon S3 est correct.
`S3_NO_SUCH_BUCKET`	Le compartiment Amazon S3 n'existe pas.	Vérifiez le nom du compartim ent et confirmez qu'il a été créé.
`S3_INVALID_OBJECT`	Artefact appartenant à Glacier ou à une classe de stockage non directement accessible.	Déplacez l'artefact vers la classe de stockage Standard.
`S3_CROSS_REGION_AC CESS_DENIED`	L'artefact se trouve dans une région différente de celle de l'image microVM.	Assurez-vous que votre artefact se trouve dans la

Erreur	Cause	Solution
		même région que votre image microVM.
`ARCHIVE_DOCKERFILE_NOT_FOUND`	Il manque un `Dockerfile` dans le répertoire racine de l'archive Zip.	Ajoutez un `Dockerfile` à la racine de votre archive zip.
`ARCHIVE_INVALID`	Le fichier d'archive n'est pas un ZIP valide ou est endommagé.	Re-create l'archive zip et retéléchargez-la.
`CONTAINER_BUILD_FAILED`	`Dockerfile` Instructions non valides, fichiers manquants ou erreurs de syntaxe.	Déboguez votre version `Dockerfile` locale à l'aide `docker build` de.
`DISK_STORAGE_FULL`	MicroVM a manqué d'espace de stockage lors de la construction.	Réduisez la taille des artefacts ou contactez l'assistance.
`INTERNAL_PLATFORM_ERROR`	Une erreur interne s’est produite.	Réessayez. Si vous persistez, contactez le support.

Résolution des problèmes liés au connecteur réseau

Code d’erreur	Cause	Solution
`DisallowedByVpcEncryptionControl`	Le VPC dispose d'une politique de contrôle du chiffrement qui empêche les interfaces réseau ou le trafic non chiffrés. Lambda ne peut pas créer d'ENI répondant aux exigences de chiffrement.	Ajoutez Lambda à la liste d'exclusion du contrôle de chiffrement VPC. Si l'exclusion n'est pas possible, utilisez un VPC ou un sous-réseau auquel aucun contrôle de chiffrement restrictif n'est appliqué.
`Ec2RequestLimitExceeded`	Lambda effectue des appels d'API EC2 (par exemple,`CreateNetworkInterface` ,`DescribeS`	Réessayez l'opération après un court laps de temps. En cas de persistance, réduisez les opération

Code d'erreur	Cause	Solution
	ubnets) pour configurer la connectivité. Un trop grand nombre d'appels d'API EC2 simultanés entraîne un ralentissement.	s simultanées du connecteur réseau ou demandez une augmentation de la limite de limitation de l'API EC2 via le support. AWS
InsufficientRolePermissions	Le rôle d'opérateur ne dispose pas des autorisations EC2 requises.	Assurez-vous que le rôle IAM dispose des autorisations réseau EC2 nécessaires.
InternalError	Une erreur inattendue s'est produite dans le service Lambda lors du traitement de la demande de connecteur réseau.	Réessayez. Si le problème persiste après plusieurs tentatives, contactez le AWS support en indiquant l'ARN du connecteur réseau et l'horodatage approximatif.
InvalidSecurityGroup	L'ID du groupe de sécurité n'existe pas, a été supprimé ou n'appartient pas au même VPC que les sous-rése aux spécifiés.	Vérifiez que tous les ID de groupe de sécurité existent et appartiennent au même VPC que les sous-réseaux. `aws ec2 describe-security-groups --group-ids <sg-id>`À utiliser pour valider.
InvalidSubnet	L'ID de sous-réseau n'existe pas, a été supprimé ou appartient à un VPC différent de celui prévu.	Vérifiez que tous les ID de sous-réseau existent et appartiennent au VPC correct. `aws ec2 describe-subnets --subnet-ids <subnet-id>` À utiliser pour valider.
SubnetOutOfIPAddresses	Le bloc CIDR du sous-réseau est épuisé : toutes les adresses IP sont attribuées aux ENI, aux instances et à d'autres ressources. Lambda ne peut donc pas créer d'interface réseau.	Libérez des adresses IP en supprimant les adresses inutilisées ENIs/instances ou utilisez un autre sous-réseau doté de la capacité disponible. Envisagez des sous-rése aux plus grands (par exemple, /24 ou plus) pour les connecteurs réseau.

Meilleures pratiques pour Lambda MicroVMS

Suivez ces bonnes pratiques pour créer des applications fiables, rentables et sécurisées avec AWS Lambda MicroVMS.

Conception de l’application

Concevez votre application pour qu'elle fonctionne correctement avec les snapshots MicroVM et les hooks de cycle de vie :

- Utilisez des hooks de cycle de vie : implémentez `/run` pour l'initialisation après l'exécution, `/suspend` pour un nettoyage en douceur, `/resume` pour le rétablissement de la connexion et pour le nettoyage des données. `/terminate`
- Gérez la réutilisation des instantanés : générez des UUID, des secrets et des valeurs aléatoires dans le `/run` hook, et non pendant la création de l'image. Utilisez CSPRNG pour toutes les générations de nombres aléatoires.
- Conception pour le CV : validez toutes les connexions réseau et l'état de la mise en cache dans le `/resume` hook. AWS Les connexions au SDK sont généralement restaurées automatiquement, mais pas nécessairement les connexions personnalisées.

Performance

Optimisez les performances de la microVM à l'aide des pratiques suivantes :

- Right-size votre microVM : choisissez la plus petite taille de microVM qui répond à vos besoins en matière de processeur, de mémoire et de bande passante. La bande passante évolue en fonction de la mémoire configurée.
- Minimisez la taille des snapshots : limitez l'encombrement de votre application afin de réduire les temps d'exécution et de reprise. Supprimez les dépendances au moment de la création et les fichiers temporaires avant la capture de l'image.
- suspend/resume À utiliser pour les charges de travail sensibles à la latence : maintenez les environnements fréquemment utilisés en état de suspension pour reprendre rapidement leur exécution.

Sécurité

Suivez ces pratiques pour sécuriser vos charges de travail microVM :

- Rotation des jetons d'authentification : générez des jetons de courte durée (15 à 30 minutes). Implémentez une logique d'actualisation des jetons dans votre client avant leur expiration.
- Portez les jetons sur des ports spécifiques : utilisez le `allowedPorts` paramètre pour limiter la portée des jetons aux seuls ports utilisés par votre application.
- Utilisez la sortie VPC pour le trafic sensible : acheminez le trafic vers les bases de données et les API internes via un connecteur de sortie VPC plutôt que vers l'Internet public.
- Appliquer l'IAM avec le moindre privilège : séparez les rôles de génération (création d'images) des rôles d'exécution (exécution). Accordez les autorisations minimales requises.

Optimisation des coûts

Réduisez les coûts grâce aux stratégies suivantes :

- Configurer les politiques d'inactivité : configurez `maxIdleDurationSeconds` pour suspendre automatiquement les micromachines virtuelles inactives. Les micromachines virtuelles suspendues n'entraînent pas de frais de calcul.
- Définissez un maximum DurationInSeconds : évitez les coûts excessifs en fixant un délai de résiliation précis pour chaque microVM.
- Mettez fin aux micromachines virtuelles inutilisées — Ne laissez pas les micromachines virtuelles fonctionner indéfiniment. Utilisez-le `suspendedDurationSeconds` pour terminer automatiquement après de longues périodes d'inactivité.
- Ressources de balises : utilisez des balises sur les images MicroVM pour la répartition des coûts et la création de rapports dans AWS Cost Explorer.
- Right-size votre microVM : commencez par la plus petite base de référence qui réponde à vos besoins en matière de performances. Vous pouvez passer à 4 fois la valeur de référence pendant les pics d'activité sans avoir à procéder à un réapprovisionnement.
- Nettoyez les images inutilisées — Supprimez les versions d'images microVM dont vous n'avez plus besoin pour réduire les coûts de stockage.

Contrôle

Surveillez efficacement vos micromachines virtuelles :

- Consultez StateReason — Lorsque des microVM se terminent de manière inattendue, la `get-microvm` réponse inclut un indiquant la raison `stateReason` de la panne inattendue.

Intégrations

AWS Lambda MicroVMS fournit des environnements informatiques isolés basés sur des instantanés que les frameworks d'agents d'intelligence artificielle et les outils de développement peuvent utiliser comme sandbox. Chaque intégration suit le même schéma : vous créez une image microVM réutilisable, et le framework lance une microVM par session ou tâche via l'API Lambda.

Les intégrations suivantes sont disponibles :

- the section called “Agents gérés par Claude”— Utilisez Lambda MicroVMS comme sandbox auto-hébergé pour les agents gérés par Claude d'Anthropic. La boucle d'agents fonctionne sur l'infrastructure d'Anthropic ; le microVM exécute vos appels d'outils. Un contrôleur piloté par webhook lance une microVM par session.
- the section called “Agents Cursor Cloud”— Utilisez les microVM Lambda comme machines auto-hébergées pour les agents Cursor Cloud. Un contrôleur planifié interroge les demandes de pool en attente et lance une microVM pour chaque session de travail.
- the section called “API OpenAI Agents”— Utilisez Lambda MicroVMS comme environnement auto-hébergé pour les agents créés avec l'API OpenAI Agents. Votre application ou un lanceur de webhook démarre une microVM à chaque tour, avec possibilité de suspension et de reprise entre les tours.

Utilisation de Lambda MicroVMS comme sandbox pour les agents gérés par Claude

AWS Lambda MicroVMS est un fournisseur de sandbox gérés dans des sandbox auto-hébergés pour Claude Managed Agents ; il conserve les fichiers, packages et services sensibles dans l'infrastructure que vous contrôlez. Anthropic héberge la boucle d'agent et le modèle Claude, tandis que la microVM Lambda est l'endroit où s'exécutent les appels de vos outils. Ce modèle vous permet

de contrôler l'environnement d'exécution : ce qui est installé, quel accès réseau est disponible et quelles ressources l'agent peut atteindre.

Chaque microVM est une machine Firecracker-isolated virtuelle dont le démarrage en moins d'une seconde est basé sur des instantanés. Elle fonctionne pendant 8 heures au maximum et peut être interrompue à la fin de la session. Les sessions ne partagent jamais l'état. Vous obtenez les limites de sécurité d'une machine virtuelle avec le modèle opérationnel sans serveur : aucun cluster à gérer, aucune capacité inactive à payer. Vous pouvez orchestrer des micromachines virtuelles avec des AWS services pour implémenter la spécification sandbox auto-hébergée, comme décrit ci-dessous. Consultez l'exemple de référence Claude Managed Agents Self-Hosted Sandbox on Lambda MicroVMS pour plus de détails.

Comment ça marche

Un plan de contrôle lance une microVM par session Claude :

1. Une session atteint l'état de fonctionnement et Anthropic envoie un `session.status_run_started` webhook à un point de terminaison de votre compte.
2. Une fonction Lambda du lanceur vérifie la signature du webhook, puis appelle. `RunMicroVM`
3. Votre code sur la microVM revendique la session, exécute des appels d'outils (bash, read, write, edit, glob, grep) et publie les résultats dans `/workspace` Anthropic.
4. La microVM est suspendue ou arrêtée à la fin de la session.

La clé d'API de votre organisation Anthropic n'atteint jamais le AWS calcul. Le lanceur transmet uniquement une référence à AWS Secrets Manager à votre clé d'environnement Anthropic ; le rôle d'exécution de la microVM permet au code de la lire au moment de l'exécution.

Principales propriétés

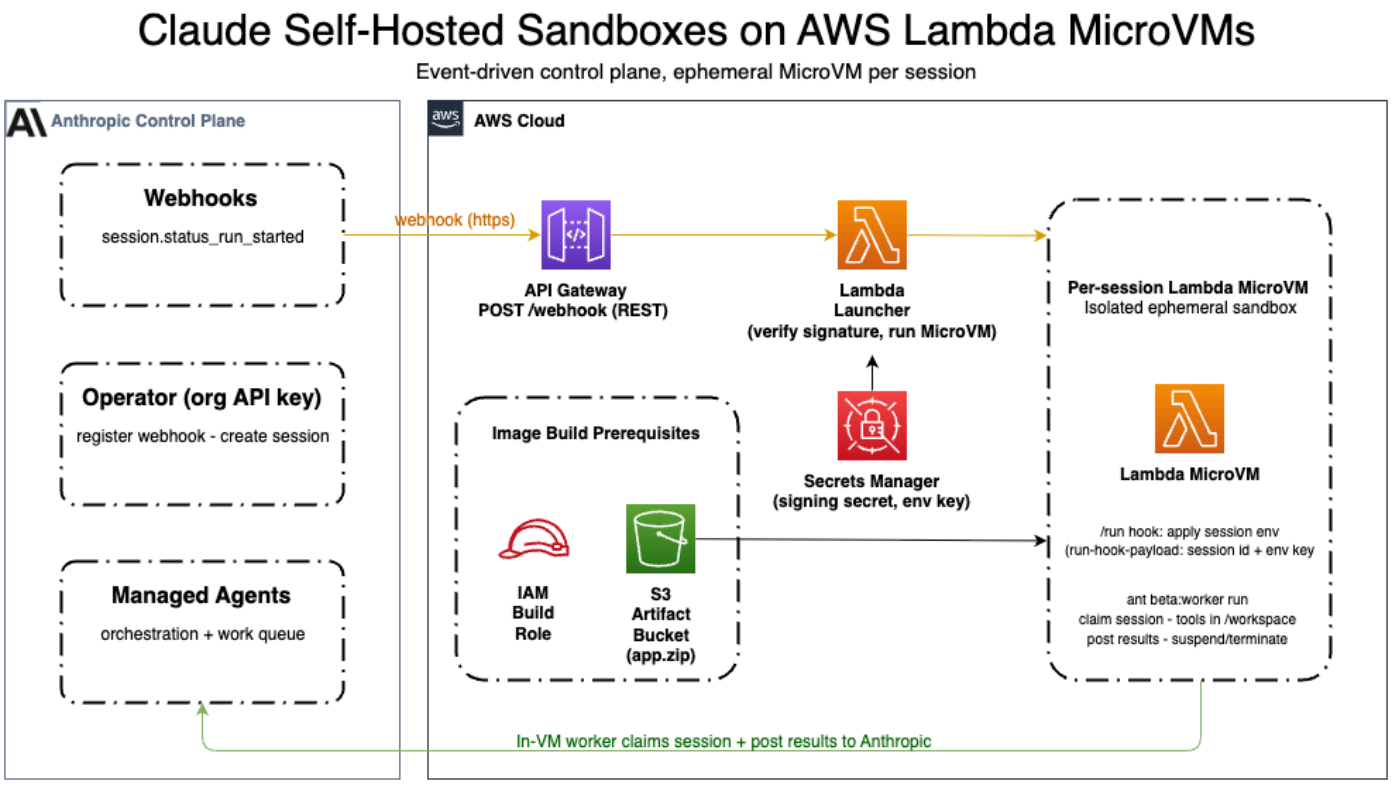
Propriété	Avantage
Isolation des pétards	Hardware-virtualized limite par session
Snapshot-based botte	Reprenez le cliché de Firecracker en moins d'une seconde à un chiffre
IAM via IMDSv2	Utilise des informations d'identification à court terme avec le moindre privilège

Propriété	Avantage
Durée avec indication	Peut fonctionner jusqu'à 8 heures avec un accès complet au disque et à la mémoire
Pay-per-session	Les micromachines virtuelles sont résiliées lorsque les sessions sont terminées, ce qui met fin à la facturation

Conditions préalables

- Un AWS compte avec des autorisations pour Amazon Simple Storage Service (Amazon S3), Gestion des identités et des accès AWS (IAM), Secrets Manager, AWS WAF, Lambda et Lambda MicroVMS
- Un agent Claude Managed Agents doté d'un `self_hosted` environnement
- Une clé d'environnement et un secret de signature du webhook provenant de la console Claude

Déploiement de l'implémentation de référence



Les Self-Hosted bacs à sable Claude Managed Agents sur le référentiel Lambda MicroVMS fournissent un déploiement fonctionnel minimal. Elle comprend les éléments suivants :

- Une CloudFormation pile (Amazon API Gateway, fonction Lambda du lanceur, secrets de Secrets Manager, compartiment Amazon S3, rôles IAM)
- Une image microVM (`Dockerfile`, Node.js EnvironmentWorker, hooks de cycle de vie)
- Un script de déploiement et un script de vérification

Étapes de déploiement :

1. Déployez la CloudFormation pile.
2. Stockez la clé d'environnement et le secret de signature dans les secrets créés par Secrets Manager.
3. Créez l'image MicroVM.
4. Enregistrez l'URL du webhook de la pile dans la console Claude.
5. Vérifiez en créant une session.

Pour des instructions détaillées, consultez le référentiel README.

Mise en réseau

Les microVM Lambda disposent d'un accès public à Internet par défaut ; aucune configuration n'est nécessaire pour y accéder. `api.anthropic.com`

Pour accéder à des ressources privées telles qu'une base de données Amazon Aurora ou un ElastiCache cluster Amazon, ou pour appliquer vos propres restrictions réseau, connectez un connecteur de sortie VPC au moment du lancement. Consultez Utilisation de connecteurs réseau de sortie.

Politique d’inactivité

Définissez `suspendedDurationSeconds: 0` et `autoResumeEnabled: false` pour les micromachines virtuelles par session. Fixé `maximumDurationInSeconds` comme plafond pour les sessions bloquées (maximum 28 800 s).

```
{
```

```
  "maxIdleDurationSeconds": 120,
  "suspendedDurationSeconds": 0,
  "autoResumeEnabled": false
}
```

Contrôle

Journaux des applications — Consultez les journaux des applications dans CloudWatch les journaux :

```
aws logs tail /aws/lambda-microvms/claude-worker --follow
```

MicroVM en cours d'exécution — Répertoriez les micromachines virtuelles en cours d'exécution dans votre compte :

```
aws lambda-microvms list-microvms \
  --image-identifier claude-worker \
  --query 'items[].[microvmId,state,startedAt]' --output table
```

Résolution des problèmes

Symptôme	Cause
Webhook renvoie 401	Signature secrète, non-concordance ou livraison périmée
Aucun lancement de microVM	Webhook non enregistré ou autorisation manquante pour `session.status_run_started` le rôle d'exécution de la fonction Lambda du lanceur `RunMicroVM`
MicroVM s'arrête immédiate ment	`/run`délai d'attente du crochet — augmentation `runTimeou tInSeconds`
Le travailleur sort immédiate ment	HTTPS sortant à bloquer `api.anthropic.com`
La création de l'image échoue `S3_*`	Configuration erronée du rôle ou du bucket dans le build

Utilisation de Lambda MicroVMS comme sandbox pour les agents Cursor Cloud

Vous pouvez utiliser les AWS Lambda microVM comme machines auto-hébergées pour vos agents Cursor Cloud, en conservant les référentiels, l'exécution des outils et l'accès au réseau dans l'infrastructure que vous contrôlez. Le curseur héberge la boucle et le modèle de l'agent ; la microVM Lambda est l'endroit où le travailleur réclame les demandes de pool et exécute les appels d'outils. Ce modèle vous permet de contrôler l'environnement d'exécution : ce qui est installé dans l'image, quel accès réseau est disponible et quelles AWS ressources le rôle IAM du collaborateur peut atteindre.

Chaque microVM est une machine Firecracker-isolated virtuelle dont le démarrage est basé sur des instantanés. Elle fonctionne pendant 8 heures au maximum et s'arrête à la fin de la session. Les sessions ne partagent jamais l'état. Vous obtenez les limites de sécurité d'une machine virtuelle avec le modèle opérationnel sans serveur : aucun cluster à gérer, aucune capacité de pool inactive à payer. Vous orchestrez les micromachines virtuelles à l'aide d'une fonction Lambda de contrôleur planifiée qui répond aux demandes de pool en attente. Consultez le modèle de référence Run self-hosted machines for Cursor Cloud Agents on AWS Lambda MicroVMS pour plus de détails.

Comment ça marche

Un contrôleur programmé lance une microVM par demande de pool en attente :

1. Vous démarrez un agent cloud au curseur. com/agentscontre une machine auto-hébergée. La demande reste en suspens jusqu'à ce qu'un travailleur la réclame.
2. La fonction Lambda du contrôleur s'exécute `agent worker controller --spawn ./spawn.sh` pendant une fenêtre de sondage Server-Sent Events (SSE) de cinq minutes. Lorsqu'il voit une demande correspondante, il s'exécute`spawn.sh`.
3. `spawn.sh`appelle `RunMicrovm` (`aws lambda-microvms run-microvm`) et revient sans attendre. Il transmet l'`CURSOR_*`environnement de la réclamation au client par le biais`--run-hook-payload`.
4. Le `/run` hook microVM (`hook.py`) applique cette charge utile et démarre`entrypoint.sh`, qui s'exécute. `cursor-agent worker --pool … start` Le travailleur exécute des appels d'outils sur votre compte.
5. Lorsque la session est inactive après l'expiration du délai de publication, le worker se libère et la microVM s'arrête.

La clé d'API de votre compte de service Cursor est stockée dans le magasin de paramètres de AWS Systems Manager en tant que fichier. `SecureString` Le contrôleur et la microVM le lisent lors de l'exécution `ssm:GetParameter` ; la clé n'est jamais intégrée à l'image.

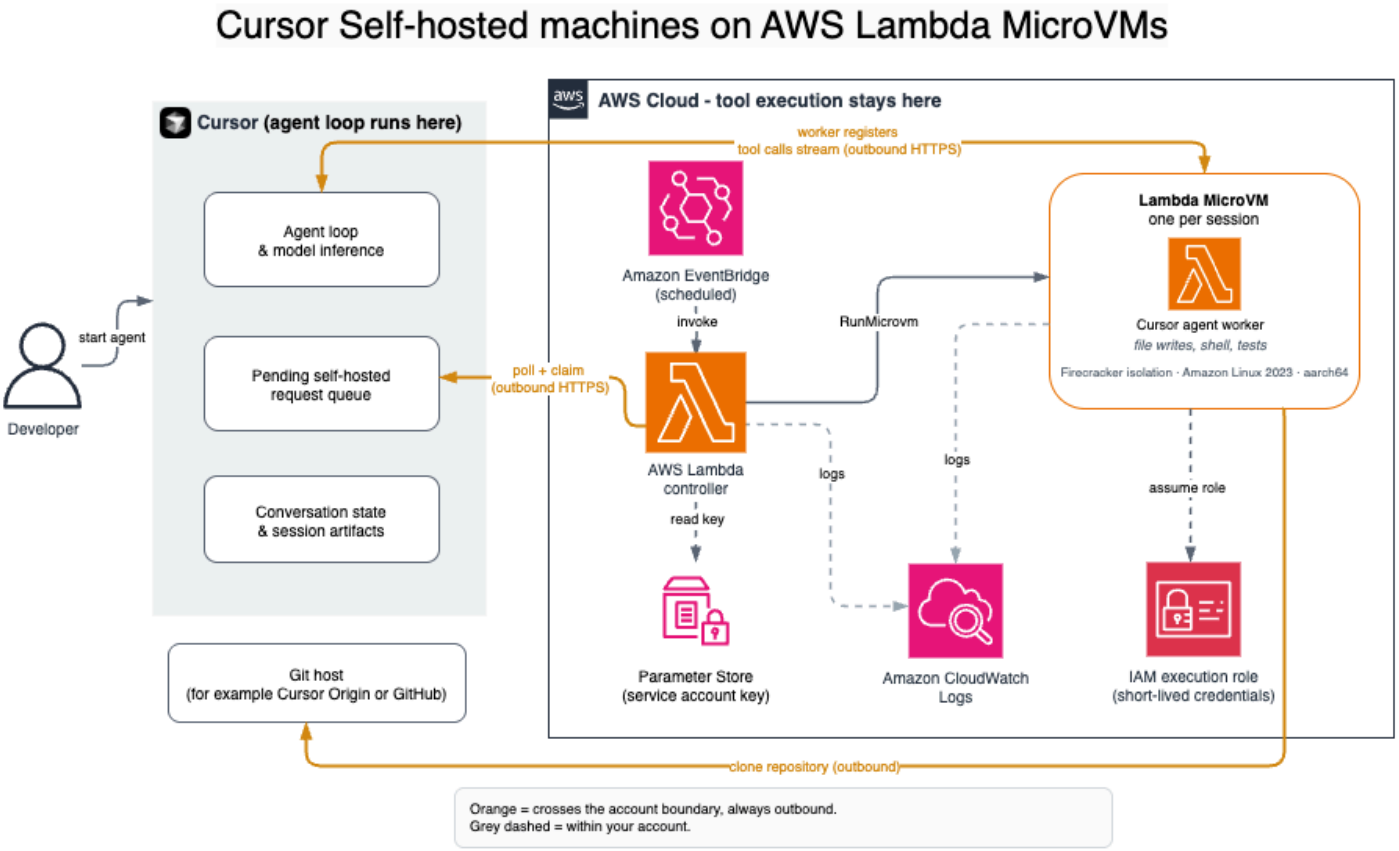
Principales propriétés

Propriété	Avantage
Isolation des pétards	Hardware-virtualized limite par session
Démarrage instantané	Lambda restaure l'invité à partir d'une capture d'écran Firecracker de votre image
L'IAM via le rôle d'exécution	L'invité utilise des informations d'identification de courte durée provenant de `MicroVmExecutionRoleArn`
Durée avec indication	Chaque microVM peut fonctionner jusqu'à 8 heures () `--maximum-duration-in-seconds 28800`
Pay-per-session	Vous payez pour le temps d'exécution d'une microVM, et non pour la capacité du pool inactif

Conditions préalables

- Un AWS compte sur lequel Lambda MicroVMS est activé et l'autorisation d'utiliser Amazon S3, IAM et Systems Manager CloudFormation Parameter Store
- Un compte Cursor Enterprise
- Une équipe Cursor avec des machines auto-hébergées activées
- Une clé d'API de compte de service pour les employés du pool
- La AWS CLI a été mise à jour vers la dernière version stable et Docker (le script de déploiement crée l'image du contrôleur)

Déploiement de l'implémentation de référence



Le référentiel anysphere/aws -lambda-workers fournit un déploiement fonctionnel minimal. Elle comprend les éléments suivants :

- Une CloudFormation pile (`cloudformation.yaml`) : une fonction Lambda du contrôleur planifié, une EventBridge `rate(1 minute)` règle, un compartiment d'artefacts Amazon S3, une file d'attente de lettres mortes et les rôles IAM (,,,) `MicroVmExecutionRole` `BuildRole` `SpawnRole` `ControllerRole`
- Une image de contrôleur (`controller/Dockerfile`,`controller/handler.py`) qui exécute une fenêtre de sondage SSE par appel
- Une image microVM (`microvm-image/`:`Dockerfile`,`hook.py`,`entrypoint.sh`)
- Un spawn hook (`spawn.sh`) et un script de déploiement () `deploy.sh`

Étapes de déploiement :

1. Enregistrez la clé d'API du compte de service dans SSM.

```
aws ssm put-parameter --type SecureString \
  --name /cursor-lambda-workers/cursor-api-key \
  --value "YOUR_SERVICE_ACCOUNT_KEY"
```

2. Déployez la pile. `deploy.sh`crée l'image du contrôleur et s'exécute`aws cloudformation deploy`.

```
POOL_NAMES=default ./deploy.sh
# POOL_NAMES=gpu,default ./deploy.sh
# ALL_POOLS=true ./deploy.sh
```

3. Créez l'image microVM à l'**`microvm-image/`**aide des sorties de la pile. Activez les crochets `validate` d'image `ready` et et le crochet `run` microVM afin qu'ils soient capturés dans le chemin du snapshot.

```
BUCKET=$(aws cloudformation describe-stacks --stack-name cursor-lambda-workers \
  --query "Stacks[0].Outputs[?OutputKey=='ArtifactBucketName'].OutputValue" --output
 text)
BUILD_ROLE=$(aws cloudformation describe-stacks --stack-name cursor-lambda-workers \
  --query "Stacks[0].Outputs[?OutputKey=='BuildRoleArn'].OutputValue" --output text)
BASE=$(aws lambda-microvms list-managed-microvm-images --query "items[0].imageArn" --
output text)
( cd microvm-image && zip -r /tmp/app.zip . )
aws s3 cp /tmp/app.zip "s3://${BUCKET}/app.zip"
aws lambda-microvms create-microvm-image \
  --code-artifact "uri=s3://${BUCKET}/app.zip" \
  --name cursor-pool-worker \
  --base-image-arn "${BASE}" \
  --build-role-arn "${BUILD_ROLE}" \
  --environment-variables "POOL_NAME=default,CURSOR_API_KEY_PARAM_NAME=/cursor-
lambda-workers/cursor-api-key" \
  --hooks '{"port":9000,"microvmImageHooks":
{"ready":"ENABLED","readyTimeoutInSeconds":60,"validate":"ENABLED","validateTimeoutInSeconds"
{"run":"ENABLED","runTimeoutInSeconds":60}}'
```

4. Démarrez un agent cloud à partir du curseur. com/agentscontre le pool (ou contre un référentiel en mode repo-bound) pour vérifier.

Pour des instructions détaillées, consultez le référentiel README.

Modes pool et repo

Gardez la pile `PoolNames` et l'image `POOL_NAME` alignées de manière à ce que la manette et l'invité servent le même pool.

- Any-repo mode — Le routage se fait par nom de pool, pas par git remote. L'invité démarre le travailleur à partir d'un espace de travail sans git remote, de sorte que le travailleur omet `repo=` les étiquettes. Les utilisateurs choisissent le nom du groupe et du pool Any repo lorsqu'ils démarrent un agent.
- Repo-bound mode — Le worker sert une ou plusieurs télécommandes Git spécifiques. Intégrez le clone dans l'image de la microVM ou configurez-le `CURSOR_REPO_URL` pour qu'il soit `entrypoint.sh` cloné au démarrage. Le worker obtient l'`repo=`étiquette à partir de la télécommande git. Les référentiels privés nécessitent des informations d'identification git sur le worker.

Mise en réseau

La référence `spawn.sh` attache le `INTERNET_EGRESS` connecteur géré afin que le travailleur puisse atteindre le plan de contrôle du curseur et `ALL_INGRESS` pour les crochets d'image. Outbound-only les travailleurs ne reçoivent jamais le protocole HTTPS entrant après le démarrage.

Pour accéder à des ressources privées (par exemple, une base de données Amazon Aurora ou un ElastiCache cluster Amazon) ou pour appliquer vos propres restrictions, connectez un connecteur de sortie VPC au moment du lancement à la place de. `INTERNET_EGRESS` Consultez the section called “Utilisation de connecteurs réseau de sortie”.

Contrôle

Journaux des invités : les journaux de MicroVM vont dans CloudWatch Logs :

```
aws logs tail /aws/lambda/microvms/cursor-pool-worker --follow
```

Journaux du contrôleur : la fonction Lambda du contrôleur se connecte à`/aws/lambda/cursor-lambda-workers-controller`.

MicroVM en cours d'exécution — Répertoriez les micromachines virtuelles en cours d'exécution pour l'image :

```
aws lambda-microvms list-microvms --image-identifier cursor-pool-worker
```

Résolution des problèmes

Symptôme	Cause
La génération de l'image échoue (S3 ou IAM)	Vérifiez les sorties de la pile `ArtifactBucketName` et `BuildRoleArn` ; le zip doit atterrir dans ce compartiment et le rôle de construction doit être capable de le lire
Aucun lancement de microVM	Le contrôleur ne fonctionne pas ou ne peut pas appeler `RunMicrovm` ; confirmez que l'`cursor-pool-worker` image existe et (pour un contrôleur local) qu'elle `SpawnRoleArn` est supposée
Le travailleur sort immédiatement	L'invité est absent `CURSOR_API_KEY` (SSM`/cursor-lambda-workers/cursor-api-key`) ou le `/run` hook n'a pas démarré `cursor-agent worker … start`
`Exec format error` sur node	L'image a installé la mauvaise architecture CLI ; les micromachines virtuelles ici sont aarch64 () `arm64`
Service-account clé signalée comme non valide	`CURSOR_API_ENDPOINT` /`CURSOR_API_URL` ont été transmis à l'invité ; ceux-ci ne doivent pas être définis et `worker start` utilisent donc l'hôte d'authentification par défaut
Image créée avant l'activation des hooks	Reconstruisez l'image de la microVM de manière `ready` à ce que les `run` hooks se trouvent dans le chemin du snapshot `validate`

Ressources connexes

- AWS MicroVM Lambda
- RunMicrovmRéférence CLI
- Démarrage rapide des machines auto-hébergées par Cursor
- Modèle de référence : anysphere/aws -lambda-workers

Utilisation de Lambda MicroVMS comme sandbox pour l'API OpenAI Agents

Vous pouvez utiliser AWS Lambda MicroVMS comme environnement auto-hébergé pour les agents créés avec l'API OpenAI Agents, en conservant les fichiers de l'espace de travail, l'exécution des outils et l'accès au réseau dans l'infrastructure que vous contrôlez. OpenAI exécute le harnais d'agents ; la microVM Lambda exécute vos tâches. Dans cet exemple, il s'exécute`codex exec-server`, qui exécute les appels d'outils de l'agent et contient les fichiers d'espace de travail de la session. Vous décidez du contenu de l'image, des chemins réseau que l'exécuteur peut emprunter et des AWS ressources auxquelles son rôle d'exécution est limité.

Chaque microVM s'exécute comme un Firecracker-isolated environnement qui démarre à partir d'un instantané de votre image. La durée de vie totale d'une microVM est de 8 heures maximum, temps de fonctionnement et de suspension compris. Terminez-le après le dernier tour ou suspendez-le entre les tours. Vous créez une image réutilisable, puis vous lancez une microVM à partir de votre application ou d'un lanceur de webhook. Les deux approches utilisent la même image et les mêmes informations d'identification. Pour plus de détails, consultez l'exemple de référence pour le sandbox auto-hébergé de l'API OpenAI Agents sur Lambda MicroVMS.

Comment ça marche

Dans le chemin géré par Webhook, une fonction Lambda du lanceur démarre une microVM lorsque la session a besoin d'un exécuteur pour la première fois. Il réutilise la microVM existante et la reprend d'abord en cas de suspension. Votre candidature y met fin après le dernier tour. La figure 1 montre le flux :

1. Votre application crée une session auto-hébergée et envoie des données à l'API Agents.
2. Lorsque la session nécessite un exécuteur, OpenAI envoie un `agent.session.action_required` webhook contenant une `environment_connection` action à un point de terminaison Amazon API Gateway de votre compte.
3. Une fonction Lambda du lanceur vérifie la signature du webhook, récupère la session en cours et confirme que le gestionnaire en est le propriétaire.
4. Le lanceur appelle `RunMicrovm` avec l'image, le rôle d'exécution, les connecteurs réseau et un élément `runHookPayload` qui contient les valeurs de connexion de la session.
5. Le `/run` hook de la microVM utilise son rôle d'exécution IAM pour récupérer la clé d'exécuteur depuis AWS Secrets Manager et démarrer Codex.

6. L'exécuteur s'enregistre auprès d'OpenAI à l'adresse. `https://api.openai.com` Il ouvre ensuite une WebSocket connexion sécurisée pour `wss://codex-cloud-environments.chatgpt.com` recevoir les commandes de l'outil et renvoyer les résultats.
7. Votre application peut charger des fichiers d'entrée et télécharger des fichiers de sortie via le point de terminaison HTTPS authentifié de la microVM. Il suit le flux d'événements de session et peut suspendre la microVM entre les tours.
8. Après le dernier tour, votre application met fin à la microVM.

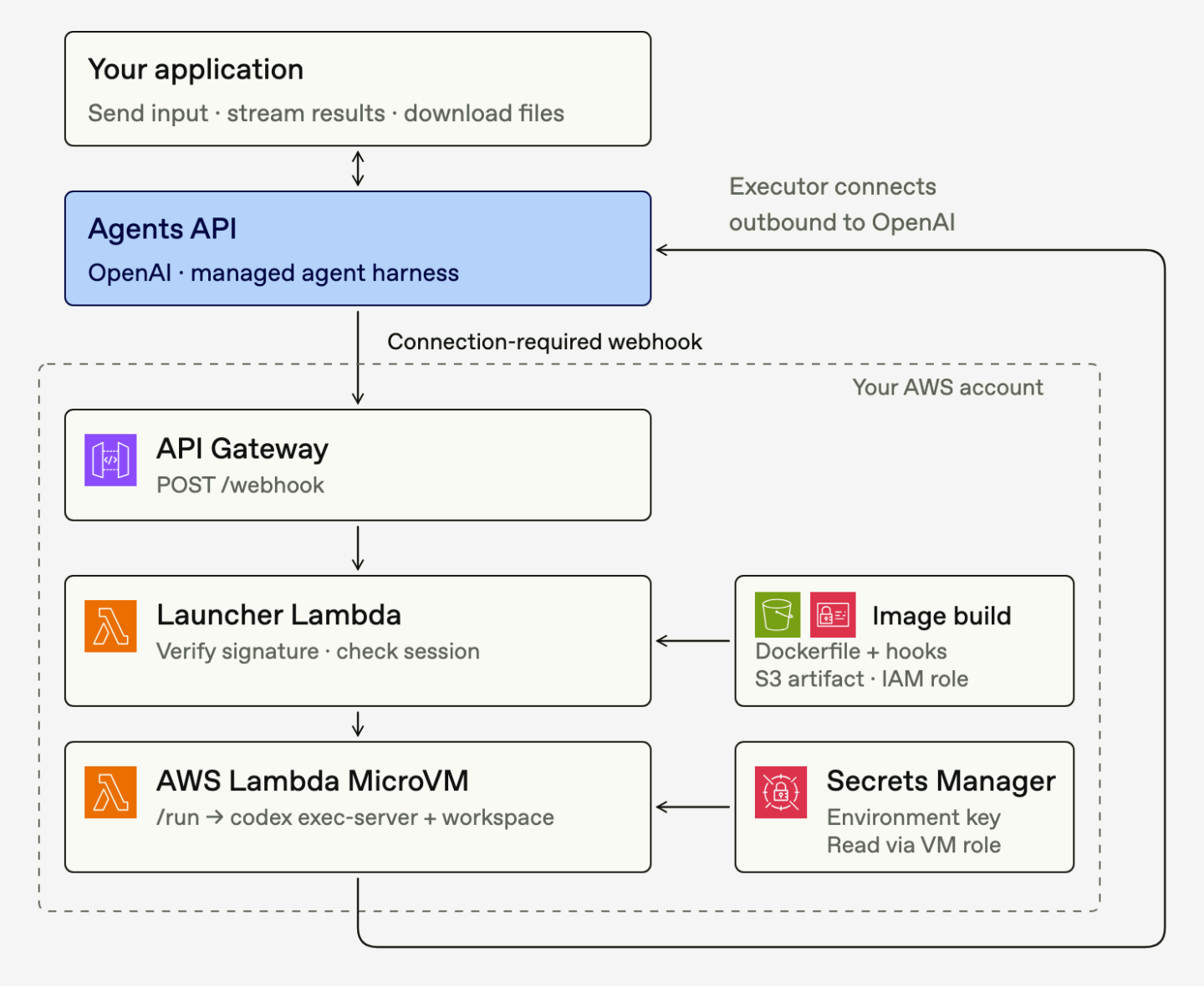


Figure 1. Webhook-managed provisionnement d'un sandbox d'API Agents sur AWS Lambda MicroVMS.

Conservez le secret de signature de la clé d'application et du webhook en dehors de la microVM. Le lanceur transmet uniquement l'ARN secret de la clé d'exécution ; la machine virtuelle récupère la clé en utilisant son rôle d'exécution.

Principales propriétés

Propriété	Avantage
Isolation des pétards	Hardware-virtualized limite pour la microVM de chaque session
Snapshot-based démarrage	Chaque microVM est lancée à partir d'un instantané de l'image que vous avez préparée
IAM via le rôle d'exécution	Le `/run` hook lit la clé de l'exécuteur avec le rôle d'exécution de la microVM ; la clé n'est pas stockée dans l'image
Durée précise	Chaque microVM peut fonctionner jusqu'à 8 heures, y compris le temps de suspension
Suspendre et reprendre entre les tours	L'état de la mémoire et du disque est préservé afin que les rotations suivantes se poursuivent dans le même environnement
Usage-based calculer	L'exécution de machines virtuelles entraîne des frais de calcul. La suspension met fin aux frais de calcul, au stockage des reads/writes instantanés et à la facturation séparée.

Conditions préalables

- Un AWS compte avec accès à Lambda MicroVMS, une version AWS CLI qui inclut `lambda-microvms` et des autorisations pour créer des images et exécuter des MicroVMS. Pour créer le compartiment d'artefacts Amazon Simple Storage Service (Amazon S3) et le rôle de création d'images Gestion des identités et des accès AWS (IAM), consultez. the section called “Créez votre première microVM”
- Une clé d'application OpenAI (`OPENAI_API_KEY`) pour créer des sessions et soumettre des informations.
- Une clé d'exécution OpenAI distincte (`OPENAI_EXECUTOR_API_KEY`) avec la même organisation, le même projet et le même compte utilisateur ou de service que la session. Stockez-le dans

Secrets Manager, par exemple sous forme de fichier`codex/agents-api/executor`. Le `/run` crochet le transmet au Codex en tant que`CODEX_API_KEY`.

- Un rôle d'exécution de microVM qui ne peut lire que le secret de la clé d'exécution. Si le secret utilise une clé du service de gestion des AWS clés (AWS AWS KMS) gérée par le client, ajoutez une autorisation de déchiffrement. Consultez the section called “Sécurité”.

Préparation de l'image MicroVM

Créez une image qui inclut la CLI Codex, les dépendances de vos outils, un répertoire de travail tel que`/workspace`, et un serveur HTTP pour les hooks du cycle de vie.

Crochet	Comportement
`/aws/lambda-microvms/runtime/v1/ready`	Renvoie le protocole HTTP 200 lorsque le serveur est prêt à permettre à Lambda de prendre le snapshot. L'exécuteur testamentaire reste déconnecté.
`/aws/lambda-microvms/runtime/v1/run`	Lit les valeurs de connexion de session et l'ARN secret, récupère la clé de l'exécuteur et démarre l'exécuteur.
`/aws/lambda-microvms/runtime/v1/validate`	Facultatif. Vérifie que Codex s'exécute et que l'espace de travail est accessible en écriture.
`/aws/lambda-microvms/runtime/v1/suspend`	Obligatoire pour suspend/resume. Arrête l'exécuteur et vide les écritures avant de créer un AWS instantané de la machine virtuelle.
`/aws/lambda-microvms/runtime/v1/resume`	Obligatoire pour suspend/resume. Récupère à nouveau la clé et redémarre l'exécuteur pour le même environnement.
`/aws/lambda-microvms/runtime/v1/terminate`	Facultatif. Arrête l'exécuteur testamentaire et efface les écritures avant la résiliation.

Emballez le serveur `Dockerfile` and hook dans un artefact Amazon S3, puis créez l'`codex-executor`image avec 8 Go de mémoire de base (4 processeurs virtuels de base). Activez les crochets sélectionnés dans la configuration de l'image et définissez le port du hook en fonction de votre serveur. Veillez à ce que les ID de session, les informations d'identification et les connexions à l'exécuteur en direct ne figurent pas dans la capture d'image. Pour la configuration de build et de hook, consultezthe section called “Images microVM”.

Au lancement, votre application ou votre lanceur sérialise les valeurs suivantes au format JSON dans `runHookPayload` :

Value	Objectif
`session.environment.id`	Identifie l'environnement auquel l'exécuteur se connecte
`session.environment.remote_url`	Fournit l'URL de connexion OpenAI de l'exécuteur
Executor-key ARN secret	Permet au hook de récupérer la clé en utilisant le rôle d'exécution de la microVM

Revenez du `/run` hook une fois que le processus d'exécution a démarré, sans attendre la fin du tour, pour éviter un délai d'expiration du hook.

Lancement de MicroVMS

Vous pouvez lancer MicroVMS depuis votre application ou depuis un lanceur de webhook. Dans les deux cas, maintenez le flux d'événements de session ouvert jusqu'à la fin du tour.

Application-managed approvisionnement

1. Créez une session auto-hébergée dont le répertoire de travail correspond à l'image, puis ouvrez son flux d'événements.
2. Appelez `RunMicrovm` avec l'ARN et la version de l'image, le rôle d'exécution, les connecteurs réseau et`runHookPayload`. Enregistrez les informations renvoyées `microvmId` à côté de l'ID de session.
3. Attendez`agent.session.environment.connected`, puis envoyez une saisie et suivez le résultat du tour.

4. Récupérez les fichiers de sortie et terminez le tour comme décrit dansthe section called “Fin d'un tour”.

Webhook-managed approvisionnement

Votre application crée la session, ouvre son flux et soumet des données. Le lanceur gère le reste lorsque le webhook arrive.

1. Déployez une `POST /webhook` route dans Amazon API Gateway qui appelle le lanceur. Accordez au lanceur l'autorisation de lire ses informations d'identification, d'inspecter, de lancer, de reprendre et d'arrêter les microVM à partir de l'image sélectionnée, de transmettre le rôle d'exécution de microVM et d'utiliser les connecteurs réseau configurés.
2. Enregistrez le point de terminaison pour `agent.session.action_required` et`agent.session.failed`. Stockez le secret de signature du terminal dans Secrets Manager à l'aide de la clé d'application du lanceur.
3. Vérifiez la signature du webhook par rapport au corps brut de la requête avant d'accéder aux sessions ou de lancer le calcul. Récupérez ensuite la session en cours et confirmez que le gestionnaire en est propriétaire, par exemple en faisant correspondre un agent enregistré dédié.
4. Si `environment_connection` c'est toujours en attente, inspectez la microVM enregistrée avec`GetMicrovm`. Reprenez-le en `ResumeMicrovm` cas de suspension. Appelez `RunMicrovm` uniquement si aucune machine virtuelle n'est enregistrée, puis enregistrez son identifiant. Si l'enregistrement échoue, arrêtez la machine virtuelle que vous avez lancée. Si l'exécuteur se connecte avant l'expiration du délai de connexion, l'entrée en attente se poursuit sans nouvelle soumission.
5. Pour un `agent.session.failed` événement, récupérez la session en cours et mettez fin à sa microVM enregistrée uniquement si son état est toujours défaillant. Ignorez les sessions supprimées, les actions résolues et les sessions appartenant à un autre gestionnaire.

L'exemple de référence enregistre l'ID de la microVM dans les métadonnées de session. Les livraisons simultanées de webhooks peuvent lancer des machines virtuelles supplémentaires avant que cet identifiant ne soit enregistré. Avant toute utilisation en production, empêchez les lancements simultanés pour la même session et dédupliquez les événements du webhook.

Fin d'un tour

La figure 2 montre le cycle de vie de la microVM pour un seul tour, ainsi que le chemin de suspension et de reprise facultatif pour les tours suivants.

Figure 2. MicroVM lifecycle for one Agents API turn

Single-turn path (solid) and multi-turn extension with suspend and resume (dashed)

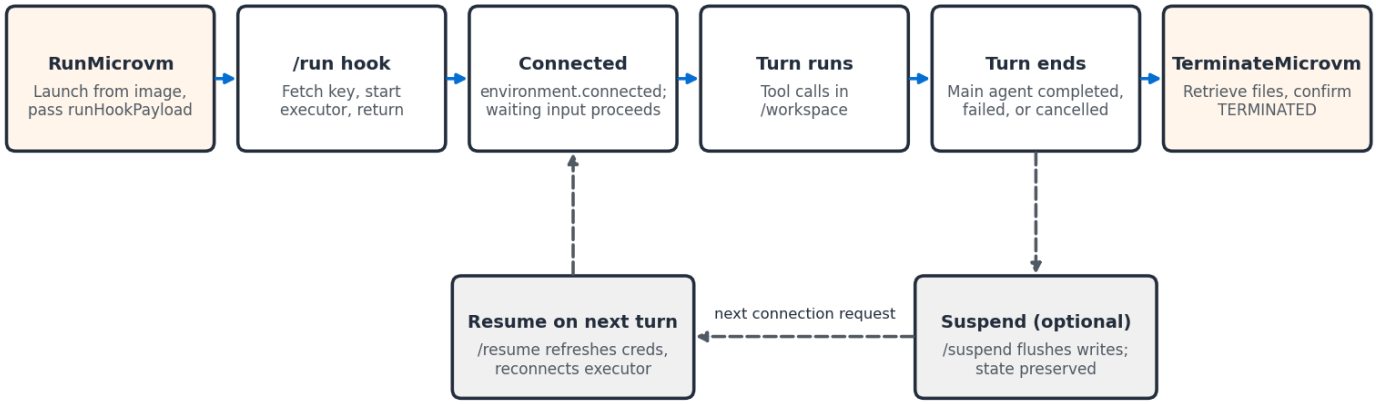


Figure 2. Cycle de vie de la microVM pour un seul tour d'API des agents. `RunMicrovm`lance la microVM, le `/run` hook démarre l'exécuteur, l'environnement se connecte, le tour s'exécute et le tour se termine. Dans le chemin en un tour de main, vous récupérez des fichiers et vous appelez`TerminateMicrovm`. Dans le chemin multitour, la microVM s'arrête après le tour et reprend à la demande de connexion suivante.

Dans le flux de session, attendez `agent.session.turn.completed`ou `agent.session.turn.failed`, ou `agent.session.turn.cancelled` l'agent principal, où se `event.turn.subagent_id` trouve`null`. Les sous-agents partagent la microVM, de sorte que les événements de leur terminal ne déclenchent pas le nettoyage. Récupérez les fichiers dont vous avez besoin. Après le dernier tour, appelez `TerminateMicrovm` et confirmez que la machine virtuelle est arrivée`TERMINATED`. Pour les tours de suivi, maintenez-le en marche ou suspendez-le. Exécutez le nettoyage si votre application rencontre une erreur.

Les résultats au tour par tour arrivent sous forme d'événements de streaming, et non d'abonnements à des webhooks. Le `agent.session.failed` webhook couvre les échecs de session, mais pas tous les tours échoués. Pour cette raison, ne vous arrêtez pas `agent.session.idle` seul, car il peut arriver avant le début de la saisie en attente.

Pour limiter la durée de vie de la microVM si le nettoyage ne s'exécute pas, configurez les paramètres suivants au lancement :

Paramètre	Conseils
`maximumDurationInSeconds`	Fixez un plafond pour la charge de travail, par exemple 900 pour un test de 15 minutes. Cette limite s'applique même lorsque les travaux sont en cours.
`maxIdleDurationSeconds`	Couvrez la charge de travail attendue. Lambda mesure le trafic entrant, de sorte que la connexion sortante de l'exécuteur ne réinitialise pas ce temporisateur.
`suspendedDurationSeconds` / `autoResumeEnabled`	Utilisez 0/false pour le modèle à tour unique, qui ne reprend pas les microVM suspendues.

Pour les commandes de durée de vie et de ralenti, voirthe section called “Exécution de microVMS”.

Supprimez la session séparément. La suppression d'une session n'arrête pas la microVM et n'envoie pas de webhook de suppression. Conservez l'image et la clé d'exécution secrètes pour les réutiliser. Pour la gestion des rotations de suivi, consultez la section Cycle de vie du https://developers.openai.com/api/docs/guides/agents-api/environments/providers/aws bac à sable.

Suspendre et reprendre entre les tours

Pour préserver la mémoire et l'état du disque entre les tours, suspendez la microVM une fois le tour de l'agent principal terminé et tous les outils et sous-agents terminés. Reprenez la même microVM la prochaine fois que la session aura besoin d'un exécuteur.

- Définissez une valeur non nulle. `suspendedDurationSeconds` Des frais de stockage des snapshots s'appliquent lorsque la microVM est suspendue.
- Activez le `/suspend` hook pour vider les écritures et fermer les connexions, et le `/resume` hook pour actualiser les informations d'identification et reconnecter l'exécuteur.
- Le chemin géré par l'application reprend la machine virtuelle avant d'envoyer l'entrée suivante. Dans le chemin géré par Webhook, l'envoi d'une entrée déclenche la demande de connexion qui relance la machine virtuelle. Le tour se poursuit une fois que l'exécuteur se reconnecte.

> **Note**
>
> `maximumDurationInSeconds`limite la durée totale de fonctionnement et de suspension à 8 heures. Pour reprendre sur demande, appelez`ResumeMicrovm`. La reprise automatique nécessite le trafic entrant vers la microVM ; la saisie de l'API Agents à elle seule ne permet pas de le reprendre.

Mise en réseau

Autorisez les connexions sortantes requises de l'exécuteur à OpenAI et à accéder à Secrets Manager. Pour accéder à des ressources privées ou appliquer vos propres restrictions réseau, connectez un connecteur de sortie VPC au moment du lancement. Consultez the section called “Utilisation de connecteurs réseau de sortie”.

L'exemple prend en charge le chargement et le téléchargement de fichiers via le point de terminaison HTTPS de la microVM, à l'aide d'un jeton d'authentification limité au port du serveur.

Contrôle

Exécutez l'un ou l'autre des exemples, puis confirmez que les `hello.txt` téléchargements atteignent `TERMINATED` la microVM et que la session supprimée renvoie HTTP 404.

Journaux du lanceur. Consultez les journaux de la fonction Lambda du lanceur dans CloudWatch Logs :

```
aws logs tail /aws/lambda/codex-agents-api-webhook --since 10m
```

Exécution de MicroVMS. Définissez `MICROVM_IMAGE_ARN` l'ARN de votre image, utilisez AWS la région de votre déploiement et répertoriez les micromachines virtuelles pour l'image :

```
aws lambda-microvms list-microvms \
  --image-identifier "$MICROVM_IMAGE_ARN" \
  --query 'items[].{id:microvmId,state:state}' --output table
```

Enregistrez les identifiants de session et de microVM ensemble afin de pouvoir suivre une exécution de bout en bout. Évitez les informations d'identification et les corps bruts des webhooks dans les journaux.

Résolution des problèmes

Symptôme	Ce qu'il faut vérifier
La signature du Webhook est rejetée	Utilisez le secret de signature du terminal et vérifiez que le corps de la demande n'a pas été modifié.
Aucun lancement de microVM	Vérifiez l'abonnement au webhook, le filtre de propriété de session, l'`environment_connection` action en attente et les autorisations IAM du lanceur.
La création de l'image échoue	Vérifiez l'artefact Amazon S3, le rôle de création de l'image et la réponse du `/ready` hook.
`/run`échoue ou expire	Vérifiez l'accès secret et le démarrage de l'exécuteur. Revenez après avoir démarré le processus, pas après le tour.
L'exécuteur ne peut pas se connecter	Vérifiez l'ID d'environnement, l'URL distante, la propriété de la clé et l'accès réseau sortant.
MicroVM s'arrête pendant un tour	Vérifiez la durée de vie maximale et la politique d'inactivité. Le trafic sortant de l'exécuteur n'est pas considéré comme une activité entrante.

En cas d'échec de connexion, inspectez les `agent.session.environment.failed` événements et les journaux de l'exécuteur. Pour le contrat d'exécuteur testamentaire partagé, voir Self-hosted sandboxes.

Ressources connexes

- MicroVM
- the section called “Exécution de microVMS”
- the section called “Sécurité”
- Référence d’API RunMicrovm
- Sandbox auto-hébergés par l'API OpenAI Agents
- Guide de l'API OpenAI Agents AWS

Sécurité dans AWS Lambda

Ce chapitre traite de la sécurité, de la gouvernance et de la conformité pour AWS Lambda. Les directives relatives à la protection des données, à la conformité, à la résilience et à la sécurité de l'infrastructure s'appliquent à tous les types de calcul Lambda. Le contrôle d'accès et le chiffrement comportent des informations spécifiques au type de calcul : pour les fonctions Web Lambda, voir, the section called “Contrôle d’accès” et the section called “Chiffrement au repos” pour les microVM Lambdathe section called “Permissions”, voir. the section called “Sécurité” Les autres rubriques de ce chapitre décrivent les fonctions d'événement Lambda.

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cette notion par les termes sécurité du cloud et sécurité dans le cloud :

- Sécurité du cloud : AWS est responsable de la protection de l'infrastructure qui fonctionne Services AWS dans le AWS cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Third-party les auditeurs testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de AWS conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à AWS Lambda, consultez Services AWS la section Portée par programme de conformité.
- Sécurité dans le cloud : votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris la sensibilité de vos données, les exigences de votre entreprise, ainsi que la législation et la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation de Lambda. Les rubriques suivantes vous montrent comment configurer Lambda pour répondre à vos objectifs de sécurité et de conformité. Vous apprendrez également à en utiliser d'autres Services AWS qui vous aident à surveiller et à sécuriser vos ressources Lambda. Les sujets abordés incluent la validation de la conformité, la protection des données, lagestion des identités et des accès, les points de terminaison VPC d'interface et la résilience.

Pour plus d'informations sur l'application de principes de sécurité aux applications Lambda, Consultez Sécurité dans Serverless Land.

Rubriques

- Protection des données dans AWS Lambda
- Utilisation de rôles liés à des services pour Lambda
- Identity and Access Management pour AWS Lambda
- Création d'une stratégie de gouvernance pour les couches et les fonctions Lambda
- Validation de conformité pour AWS Lambda
- Résilience dans AWS Lambda
- Sécurité de l'infrastructure dans AWS Lambda
- Sécurisation des charges de travail avec des points de terminaison publics
- Utilisation de la signature de code pour vérifier l'intégrité du code avec Lambda

Protection des données dans AWS Lambda

> **Note**
>
> Les détails du chiffrement présentés dans cette rubrique, y compris le chiffrement des variables d'environnement, décrivent les fonctions d'événement Lambda. Pour le chiffrement des fonctions Web Lambda, voir. the section called "Chiffrement au repos"

Le modèle de responsabilité partagée AWS s'applique à la protection des données dans AWS Lambda. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez la FAQ sur la confidentialité des données et les . Pour plus d'informations sur la protection des données en Europe, consultez le Centre du règlement général sur la protection des données (RGPD).

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou Gestion des identités et des accès AWS (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l’authentification multifactorielle (MFA) avec chaque compte.
- SSL/TLS À utiliser pour communiquer avec AWS les ressources. Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail. Pour plus d'informations sur l'utilisation des CloudTrail sentiers pour capturer AWS des activités, consultez la section Utilisation des CloudTrail sentiers dans le guide de AWS CloudTrail l'utilisateur.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu’Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-3 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d’informations sur les points de terminaison FIPS disponibles, consultez Norme FIPS (Federal Information Processing Standard) 140-3.

Nous vous recommandons fortement de ne jamais placer d’informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Nom. Cela inclut lorsque vous travaillez avec Lambda ou d'autres utilisateurs à Services AWS l'aide de la console, de l'API ou AWS des AWS CLI SDK. Toutes les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d’informations d’identification dans l’adresse URL permettant de valider votre demande adressée à ce serveur.

Sections

- Chiffrement en transit
- Chiffrement des données au repos pour AWS Lambda

Chiffrement en transit

Les points de terminaison d’API Lambda ne prennent en charge que des connexions sécurisées sur HTTPS. Lorsque vous gérez les ressources Lambda à l'aide du AWS SDK Console de gestion AWS ou de l'API Lambda, toutes les communications sont cryptées avec le protocole TLS (Transport Layer Security). Pour obtenir la liste complète des points de terminaison d’API, consultez Régions et points de terminaison AWS dans Références générales AWS.

Lorsque vous connectez votre fonction à un système de fichiers, Lambda utilise le chiffrement pendant le transit pour toutes les connexions. Pour en savoir plus, consultez Chiffrement des données dans Amazon EFS que vous trouverez dans le guide de l'utilisateur Amazon Elastic File System.

Lorsque vous utilisez variables d'environnement, vous pouvez activer les assistants de chiffrement de la console afin qu'ils utilisent le chiffrement côté client pour protéger les variables d'environnement en transit. Pour plus d'informations, consultez Sécurisation de variables d'environnement Lambda.

Chiffrement des données au repos pour AWS Lambda

AWS Lambda fournit toujours un chiffrement au repos pour les ressources suivantes :

- Variables d'environnement
- Les fichiers que vous chargez sur Lambda, y compris les packages de déploiement et les archives de couches
- Les objets de critères de filtre de mappage des sources d'événements
- Données d'exécution durables

> **Note**
>
> Pour les fonctions et les couches qui utilisent le stockage de code S3 autogéré, Lambda ne stocke aucune copie de votre code source. Votre code reste dans votre compartiment S3, et le chiffrement au repos de votre code source est géré par la configuration de votre compartiment S3. Lambda utilisera `KMSKeyArn` pour chiffrer la version décompressée du package que Lambda utilise pour appeler la fonction. Pour plus d'informations, consultez la section Protection des données avec le chiffrement côté serveur dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Vous pouvez éventuellement configurer Lambda pour utiliser une clé gérée par le client afin de chiffrer vos variables d'environnement, vos packages de déploiement .zip, vos objets de critères de filtrage et vos données d'exécution durables.

Amazon CloudWatch Logs chiffre AWS X-Ray également les données par défaut et peut être configuré pour utiliser une clé gérée par le client. Pour plus de détails, voir Chiffrer les données des CloudWatch journaux dans les journaux et Protection des données dans AWS X-Ray.

Surveillance de vos clés de chiffrement pour Lambda

Lorsque vous utilisez une clé gérée par AWS KMS le client avec Lambda, vous pouvez utiliser. AWS CloudTrail Les exemples suivants sont CloudTrail des événements et des `GenerateDataKey` appels effectués par Lambda pour `Decrypt` accéder à des données chiffrées par votre clé gérée par le client. `DescribeKey`

Pour CloudTrail des exemples spécifiques aux données d'exécution durables, voirSurveillance des clés KMS pour des fonctions durables.

Decrypt

Si vous avez utilisé une clé gérée par le AWS KMS client pour chiffrer votre objet de critères de filtrage, Lambda envoie `Decrypt` une demande en votre nom lorsque vous essayez d'y accéder en texte clair (par exemple, depuis `ListEventSourceMappings` un appel). L'exemple d'événement suivant enregistre l'opération `Decrypt` :


```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROA123456789EXAMPLE:example",
        "arn": "arn:aws:sts::123456789012:assumed-role/role-name/example",
        "accountId": "123456789012",
        "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROA123456789EXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/role-name",
                "accountId": "123456789012",
                "userName": "role-name"
            },
            "attributes": {
                "creationDate": "2024-05-30T00:45:23Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "lambda.amazonaws.com"
    },
    "eventTime": "2024-05-30T01:05:46Z",
    "eventSource": "kms.amazonaws.com",
```

```
    "eventName": "Decrypt",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "lambda.amazonaws.com",
    "userAgent": "lambda.amazonaws.com",
    "requestParameters": {
        "keyId": "arn:aws:kms:eu-west-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
        "encryptionContext": {
            "aws-crypto-public-key": "ABCD
+7876787678+CDEFGHIJKL/888666888999888555444111555222888333111==",
            "aws:lambda:EventSourceArn": "arn:aws:sqs:eu-west-1:123456789012:sample-
source",
            "aws:lambda:FunctionArn": "arn:aws:lambda:eu-
west-1:123456789012:function:sample-function"
        },
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
    },
    "responseElements": null,
    "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa",
    "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLEbbbbb",
    "readOnly": true,
    "resources": [
        {
            "accountId": "AWS Internal",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-west-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "sessionCredentialFromConsole": "true"
}
```

DescribeKey

Si vous avez utilisé une clé gérée par le AWS KMS client pour chiffrer votre objet de critères de filtre, Lambda envoie `DescribeKey` une demande en votre nom lorsque vous essayez d'y accéder (par exemple, depuis `GetEventSourceMapping` un appel). L'exemple d'événement suivant enregistre l'opération `DescribeKey` :

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROA123456789EXAMPLE:example",
        "arn": "arn:aws:sts::123456789012:assumed-role/role-name/example",
        "accountId": "123456789012",
        "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROA123456789EXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/role-name",
                "accountId": "123456789012",
                "userName": "role-name"
            },
            "attributes": {
                "creationDate": "2024-05-30T00:45:23Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2024-05-30T01:09:40Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DescribeKey",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "54.240.197.238",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36",
    "requestParameters": {
        "keyId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
    },
    "responseElements": null,
    "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa",
    "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLEbbbbb",
    "readOnly": true,
    "resources": [
        {
            "accountId": "AWS Internal",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-west-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
        }
```

```
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_256_GCM_SHA384",
        "clientProvidedHostHeader": "kms.eu-west-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}
```

GenerateDataKey

Lorsque vous utilisez une clé gérée par le AWS KMS client pour chiffrer l'objet de vos critères de filtre dans un `UpdateEventSourceMapping` appel `CreateEventSourceMapping` OR, Lambda envoie `GenerateDataKey` une demande en votre nom pour générer une clé de données afin de chiffrer les critères de filtre (chiffrement d'enveloppe). L'exemple d'événement suivant enregistre l'opération `GenerateDataKey` :

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROA123456789EXAMPLE:example",
        "arn": "arn:aws:sts::123456789012:assumed-role/role-name/example",
        "accountId": "123456789012",
        "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROA123456789EXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/role-name",
                "accountId": "123456789012",
                "userName": "role-name"
            },
            "attributes": {
                "creationDate": "2024-05-30T00:06:07Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "lambda.amazonaws.com"
```

```
    },
    "eventTime": "2024-05-30T01:04:18Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "lambda.amazonaws.com",
    "userAgent": "lambda.amazonaws.com",
    "requestParameters": {
        "numberOfBytes": 32,
        "keyId": "arn:aws:kms:eu-west-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
        "encryptionContext": {
            "aws-crypto-public-key": "ABCD
+7876787678+CDEFGHIJKL/888666888999888555444111555222888333111==",
            "aws:lambda:EventSourceArn": "arn:aws:sqs:eu-west-1:123456789012:sample-
source",
            "aws:lambda:FunctionArn": "arn:aws:lambda:eu-
west-1:123456789012:function:sample-function"
        },
    },
    "responseElements": null,
    "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa",
    "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLEbbbbb",
    "readOnly": true,
    "resources": [
        {
            "accountId": "AWS Internal",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-west-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```


Utilisation de rôles liés à des services pour Lambda

Lambda utilise des rôles Gestion des identités et des accès AWS liés à des services (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à Lambda. Service-linked les rôles

sont prédéfinis par Lambda et incluent les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom.

Lambda définit les autorisations de ses rôles liés aux services, et seul Lambda peut assumer ses rôles. Les autorisations définies comprennent la politique de confiance et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Vous pouvez supprimer un rôle lié à un service uniquement après la suppression préalable de ses ressources connexes. Cela protège vos ressources Lambda car vous ne pouvez pas supprimer par inadvertance l'autorisation d'accès aux ressources.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés aux services, consultez la section AWS Services qui fonctionnent avec IAM et recherchez les services dont la valeur est Oui dans la Service-linked colonne des rôles. Choisissez un Oui ayant un lien permettant de consulter les détails du rôle pour ce service.

Service-linked autorisations de rôle pour Lambda

Lambda utilise le rôle lié à un service nommé. AWSServiceRoleForLambda Le rôle lié à un service approuve les services suivants pour endosser le rôle :

- `lambda.amazonaws.com`

La politique d'autorisations de rôle nommée AWSLambdaServiceRolePolicy permet à Lambda d'effectuer les actions suivantes sur les ressources spécifiées :

- Action : `ec2:TerminateInstances` continuer `arn:aws:ec2:*:*:instance/*` avec la condition qui `ec2:ManagedResourceOperator` est égale `scaler.lambda.amazonaws.com`
- Action : `ec2:DescribeInstanceStatus` et `ec2:DescribeInstances` sur `*`

Vous devez configurer les autorisations de manière à permettre à vos utilisateurs, groupes ou rôles de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez la section sur les autorisations relatives aux Service-linked rôles dans le guide de l'utilisateur IAM.

Pour les mises à jour des politiques gérées, consultez la section Politiques gérées Lambda.

Création d'un rôle lié à un service pour Lambda

Vous n’avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous créez un fournisseur de capacité Lambda dans l' Console de gestion AWS AWS API AWS CLI, Lambda crée le rôle lié au service pour vous.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous créez un fournisseur de capacité Lambda, Lambda crée à nouveau le rôle lié au service pour vous.

Vous pouvez également utiliser la console IAM pour créer un rôle lié à un service avec le AWSServiceRoleForLambda cas d'utilisation. Dans l'API AWS CLI ou l' AWS API, créez un rôle lié à un service avec le nom du `lambda.amazonaws.com` service. Pour plus d’informations, consultez Création d’un rôle lié à un service dans le Guide de l’utilisateur IAM. Si vous supprimez ce rôle lié à un service, vous pouvez utiliser ce même processus pour créer le rôle à nouveau.

Modification d'un rôle lié à un service pour Lambda

Lambda ne vous permet pas de modifier le rôle lié à un AWSServiceRoleForLambda service. Après avoir créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez modifier la description du rôle à l’aide d’IAM. Pour plus d’informations, consultez Modification d’un rôle lié à un service dans le Guide de l’utilisateur IAM.

Supprimer un rôle lié à un service pour Lambda

Si vous n’avez plus besoin d’utiliser une fonction ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n’avez aucune entité inutilisée qui n’est pas surveillée ou gérée activement. Cependant, vous devez nettoyer les ressources de votre rôle lié à un service avant de pouvoir les supprimer manuellement.

> **Note**
>
> Si le service Lambda utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression peut échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer les ressources Lambda utilisées par AWSServiceRoleForLambda

1. Supprimez tous les fournisseurs de capacité Lambda de votre compte. Vous pouvez le faire à l'aide de la console Lambda, de l'interface de ligne de commande ou de l'API.
2. Vérifiez qu'aucun fournisseur de capacité Lambda n'est présent dans votre compte avant de tenter de supprimer le rôle lié au service.

Pour supprimer manuellement le rôle lié au service à l’aide d’IAM

Utilisez la console IAM AWS CLI, l'API ou l' AWS API pour supprimer le rôle lié au AWSServiceRoleForLambda service. Pour plus d’informations, consultez la section Suppression d’un rôle lié à un service dans le Guide de l’utilisateur IAM.

Régions prises en charge pour les rôles liés aux services Lambda

Lambda ne prend pas en charge l'utilisation de rôles liés à un service dans toutes les régions où le service est disponible. AWSServiceRoleForLambda est pris en charge dans les régions suivantes.

Nom de la région	Identité de la région	Assistance dans Lambda
USA Est (Virginie du Nord)	us-east-1	Oui
USA Est (Ohio)	us-east-2	Oui
USA Ouest (Californie du Nord)	us-west-1	Oui
USA Ouest (Oregon)	us-west-2	Oui
Afrique (Le Cap)	af-south-1	Non
Asie-Pacifique (Hong Kong)	ap-east-1	Oui
Asie-Pacifique (Jakarta)	ap-southeast-3	Oui
Asie-Pacifique (Bangkok)	ap-southeast-7	Oui
Asie-Pacifique (Mumbai)	ap-south-1	Oui
Asie-Pacifique (Osaka)	ap-northeast-3	Non

Nom de la région	Identité de la région	Assistance dans Lambda
Asie-Pacifique (Séoul)	ap-northeast-2	Non
Asie-Pacifique (Singapour)	ap-southeast-1	Oui
Asie-Pacifique (Sydney)	ap-southeast-2	Oui
Asie-Pacifique (Tokyo)	ap-northeast-1	Oui
Canada (Centre)	ca-central-1	Non
Europe (Francfort)	eu-central-1	Oui
Europe (Irlande)	eu-west-1	Oui
Europe (Londres)	eu-west-2	Oui
Europe (Milan)	eu-south-1	Non
Europe (Paris)	eu-west-3	Non
Europe (Stockholm)	eu-north-1	Non
Moyen-Orient (Bahreïn)	me-south-1	Non
Moyen-Orient (EAU)	me-central-1	Non
Amérique du Sud (São Paulo)	sa-east-1	Non
AWS GovCloud (US-East)	us-gov-east-1	Non
AWS GovCloud (US-West)	us-gov-west-1	Non

Identity and Access Management pour AWS Lambda

> **Note**
>
> Les directives de politique basées sur l'identité et les ressources présentées dans cette rubrique décrivent les fonctions d'événement Lambda. Les fonctions Web Lambda utilisent

un modèle de contrôle d'accès différent ; voir et. the section called “Permissions” the section called “Contrôle d’accès” Pour les microVM Lambda, voir. the section called “Sécurité”

Gestion des identités et des accès AWS (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Des administrateurs IAM contrôlent les personnes qui s’authentifient (sont connectées) et sont autorisées (disposent d’autorisations) à utiliser des ressources . IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

- Public ciblé
- Authentification par des identités
- Gestion de l’accès à l’aide de politiques
- Comment ? AWS Lambda fonctionne avec IAM
- Identity-based exemples de politiques pour AWS Lambda
- AWS politiques gérées pour AWS Lambda
- Résolution des problèmes AWS Lambda identité et accès

Public ciblé

La façon dont vous utilisez Gestion des identités et des accès AWS (IAM) varie en fonction de votre rôle :

- Utilisateur du service : demandez des autorisations à votre administrateur si vous ne pouvez pas accéder aux fonctionnalités (voir Résolution des problèmes AWS Lambda identité et accès)
- Administrateur du service : déterminez l’accès des utilisateurs et soumettez les demandes d’autorisation (voir Comment ? AWS Lambda fonctionne avec IAM)
- Administrateur IAM : rédigez des politiques pour gérer l’accès (voir Identity-based exemples de politiques pour AWS Lambda)

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en tant qu'identité fédérée à l'aide d'informations d'identification provenant d'une source d'identité telle que AWS IAM Identity Center (IAM Identity Center), d'une authentification unique ou d'informations d'identification. Google/Facebook Pour plus d'informations sur la connexion, consultez Connexion à votre Compte AWS dans le Guide de l'utilisateur Connexion à AWS .

Pour l'accès par programmation, AWS fournit un SDK et une CLI pour signer les demandes de manière cryptographique. Pour plus d'informations, consultez Signature AWS Version 4 pour les demandes d'API dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une seule identité de connexion appelée utilisateur Compte AWS root qui dispose d'un accès complet à toutes Services AWS les ressources. Il est vivement déconseillé d'utiliser l'utilisateur racine pour vos tâches quotidiennes. Pour les tâches qui requièrent des informations d'identification de l'utilisateur racine, consultez Tâches qui requièrent les informations d'identification de l'utilisateur racine dans le Guide de l'utilisateur IAM.

Identité fédérée

Il est recommandé d'obliger les utilisateurs humains à utiliser la fédération avec un fournisseur d'identité pour accéder à Services AWS l'aide d'informations d'identification temporaires.

Une identité fédérée est un utilisateur provenant de l'annuaire de votre entreprise, de votre fournisseur d'identité Web ou Directory Service qui y accède à Services AWS l'aide d'informations d'identification provenant d'une source d'identité. Les identités fédérées assument des rôles qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Pour plus d'informations, consultez Qu'est-ce que IAM Identity Center ? dans le Guide de l'utilisateur AWS IAM Identity Center .

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité qui dispose d'autorisations spécifiques pour une seule personne ou application. Nous vous recommandons d'utiliser ces informations d'identification temporaires au lieu des utilisateurs IAM avec des informations d'identification à long terme. Pour plus d'informations, voir Exiger des utilisateurs humains qu'ils utilisent la fédération avec un fournisseur d'identité pour accéder à AWS l'aide d'informations d'identification temporaires dans le guide de l'utilisateur IAM.

Les groupes IAM spécifient une collection d'utilisateurs IAM et permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Pour plus d'informations, consultez Cas d'utilisation pour les utilisateurs IAM dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité dotée d'autorisations spécifiques qui fournit des informations d'identification temporaires. Vous pouvez assumer un rôle en passant d'un rôle d'utilisateur à un rôle IAM (console) ou en appelant une opération d' AWS API AWS CLI ou d'API. Pour plus d'informations, consultez Méthodes pour endosser un rôle dans le Guide de l'utilisateur IAM.

Les rôles IAM sont utiles pour l'accès des utilisateurs fédérés, les autorisations temporaires des utilisateurs IAM, les accès intercompte, les accès entre services et les applications exécutées sur Amazon EC2. Pour plus d'informations, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Gestion de l'accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique définit les autorisations lorsqu'elles sont associées à une identité ou à une ressource. AWS évalue ces politiques lorsqu'un directeur fait une demande. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations les documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

À l'aide de politiques, les administrateurs précisent qui a accès à quoi en définissant quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Un administrateur IAM crée des politiques IAM et les ajoute aux rôles, que les utilisateurs peuvent ensuite assumer. Les politiques IAM définissent les autorisations quelle que soit la méthode que vous utilisez pour exécuter l'opération.

Identity-based politiques

Identity-based les politiques sont des documents de politique d'autorisation JSON que vous attachez à une identité (utilisateur, groupe ou rôle). Ces politiques contrôlent les actions que peuvent exécuter ces identités, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Définition d'autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l'utilisateur IAM.

Identity-based les politiques peuvent être des politiques intégrées (intégrées directement dans une seule identité) ou des politiques gérées (politiques autonomes associées à plusieurs identités). Pour découvrir comment choisir entre des politiques gérées et en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

Resource-based politiques

Resource-based les politiques sont des documents de politique JSON que vous attachez à une ressource. Les exemples incluent les politiques de confiance de rôle IAM et les stratégies de compartiment Amazon S3. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Vous devez spécifier un principal dans une politique basée sur les ressources.

Resource-based les politiques sont des politiques intégrées qui se trouvent dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Autres types de politique

AWS prend en charge des types de politiques supplémentaires qui peuvent définir les autorisations maximales accordées par les types de politiques les plus courants :

- Limites d'autorisations : une limite des autorisations définit le nombre maximum d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM. Pour plus d'informations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.
- Politiques de contrôle des services (SCP) : spécifient les autorisations maximales pour une organisation ou une unité organisationnelle dans AWS Organizations. Pour plus d'informations, consultez Politiques de contrôle de service dans le Guide de l'utilisateur AWS Organizations .
- Politiques de contrôle des ressources (RCP) : définissent les autorisations maximales disponibles pour les ressources de votre organisation. Pour plus d'informations, consultez Politiques de contrôle des ressources (RCP) dans le Guide de l'utilisateur AWS Organizations .

- Politiques de session : politiques avancées que vous passez en tant que paramètre lorsque vous créez par programmation une session temporaire pour un rôle ou un utilisateur fédéré. Pour plus d'informations, consultez Politiques de session dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

Comment ? AWS Lambda fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès à Lambda, découvrez les fonctions IAM que vous pouvez utiliser avec Lambda.

Fonctionnalité IAM	Support Lambda
Identity-based politiques	Oui
Resource-based politiques	Oui
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition de politique (spécifiques au service)	Oui
ACL	Non
ABAC (identifications dans les politiques)	Partielle
Informations d'identification temporaires	Oui
Transfert des sessions d'accès (FAS)	Non
Rôles de service	Oui

Fonctionnalité IAM	Support Lambda
Service-linked rôles	Partielle

Pour obtenir une vue d'ensemble de la façon dont Lambda et les autres AWS services fonctionnent avec la plupart des fonctionnalités IAM, consultez la section AWS Services compatibles avec IAM dans le guide de l'utilisateur IAM.

Identity-based politiques pour Lambda

Prend en charge les politiques basées sur l’identité : oui

Identity-based les politiques sont des documents de politique d'autorisation JSON que vous pouvez associer à une identité, telle qu'un utilisateur IAM, un groupe d'utilisateurs ou un rôle. Ces politiques contrôlent quel type d’actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l’identité, consultez Définition d’autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l’utilisateur IAM.

Avec les politiques IAM basées sur l’identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Pour découvrir tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l’utilisateur IAM.

Identity-based exemples de politiques pour Lambda

Pour voir des exemples de politiques Lambda basées sur l’identité, consultez Identity-based exemples de politiques pour AWS Lambda.

Resource-based politiques au sein de Lambda

Prend en charge les politiques basées sur les ressources : oui

Resource-based les politiques sont des documents de politique JSON que vous attachez à une ressource. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l’accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d’actions un principal spécifié peut effectuer sur cette ressource

et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. Pour plus d'informations, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Vous pouvez attacher une politique basée sur les ressources à une fonction ou une couche Lambda. Cette politique désigne les principaux autorisés à effectuer des actions sur la fonction ou la couche.

Pour savoir comment attacher une politique basée sur les ressources à une fonction ou une couche, consultez Utilisation de politiques basées sur les ressources dans Lambda.

Actions de politique pour Lambda

Prend en charge les actions de politique : oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Intégration d'actions dans une politique afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour afficher la liste des actions Lambda, consultez Actions définies par AWS Lambda dans la Référence de l'autorisation de service.

Les actions de politique dans Lambda utilisent le préfixe suivant avant l'action :

```
lambda
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

```
"Action": [
      "lambda:action1",
      "lambda:action2"
         ]
```

Pour voir des exemples de politiques Lambda basées sur l'identité, consultez Identity-based exemples de politiques pour AWS Lambda.

Ressources de politique pour Lambda

Prend en charge les ressources de politique : oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

Pour afficher la liste des types de ressources Lambda et leurs ARN, consultez Types de ressources définies par AWS Lambda dans la Référence de l'autorisation de service. Pour savoir grâce à quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez Actions définies par AWS Lambda.

Pour voir des exemples de politiques Lambda basées sur l'identité, consultez Identity-based exemples de politiques pour AWS Lambda.

Clés de condition de politique pour Lambda

Prend en charge les clés de condition de politique spécifiques au service : oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` indique à quel moment les instructions s'exécutent en fonction de critères définis. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

Pour afficher la liste des clés de condition Lambda, consultez Clés de condition pour AWS Lambda dans la Référence de l'autorisation de service. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez la section Actions définies par AWS Lambda.

Pour voir des exemples de politiques Lambda basées sur l'identité, consultez Identity-based exemples de politiques pour AWS Lambda.

Listes ACL dans Lambda

Prend en charge les ACL : non

Les listes de contrôle d'accès (ACL) vérifie quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

ABAC avec Lambda

Prend en charge ABAC (identifications dans les politiques) : partiellement

Attribute-based le contrôle d'accès (ABAC) est une stratégie d'autorisation qui définit les autorisations en fonction d'attributs appelés balises. Vous pouvez associer des balises aux entités et aux AWS ressources IAM, puis concevoir des politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de la ressource.

Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informations sur ABAC, consultez Définition d'autorisations avec l'autorisation ABAC dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l'ABAC, consultez Utilisation du contrôle d'accès par attributs (ABAC) dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur le balisage des ressources Lambda, consultez Utilisation du contrôle d'accès basé sur les attributs dans Lambda.

Utilisation des informations d’identification temporaires avec Lambda

Prend en charge les informations d’identification temporaires : oui

Les informations d'identification temporaires fournissent un accès à court terme aux AWS ressources et sont automatiquement créées lorsque vous utilisez la fédération ou que vous changez de rôle. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d’informations, consultez Informations d’identification de sécurité temporaires dans IAM et Services AWS compatibles avec IAM dans le Guide de l’utilisateur IAM.

Transmission des sessions d’accès pour Lambda

Prend en charge les sessions d’accès direct (FAS) : oui

Les sessions d'accès direct (FAS) utilisent les autorisations du principal appelant et Service AWS, combinées Service AWS à la demande d'envoi de demandes aux services en aval. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez la section Sessions de transmission d’accès.

Rôles de service pour Lambda

Prend en charge les rôles de service : oui

Un rôle de service est un rôle IAM qu’un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer un rôle de service à partir d’IAM. Pour plus d’informations, consultez Création d’un rôle pour la délégation d’autorisations à un Service AWS dans le Guide de l’utilisateur IAM.

Dans Lambda, un rôle de service est appelé rôle d’exécution.

> **Warning**
>
> La modification des autorisations d’un rôle d’exécution peut altérer la fonction Lambda.

Service-linked rôles pour Lambda

Prend en charge les rôles liés à un service : partiellement

Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut assumer le rôle d'effectuer une action en votre nom. Service-linked les rôles apparaissent dans votre fichier Compte AWS et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Lambda n'a pas de rôles liés au service, contrairement à Lambda@Edge. Pour plus d'informations, consultez la section Service-Linked Rôles pour Lambda @Edge dans le manuel Amazon CloudFront Developer Guide.

Pour plus d'informations sur la création ou la gestion des rôles liés à un service, consultez Services AWS qui fonctionnent avec IAM. Recherchez un service dans le tableau qui inclut un `Yes` dans la colonne des Service-linked rôles. Choisissez le lien Oui pour consulter la documentation du rôle lié à ce service.

Identity-based exemples de politiques pour AWS Lambda

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier des ressources Lambda. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez Création de politiques IAM (console) dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par Lambda, y compris le format des ARN pour chacun des types de ressources, veuillez consulter la rubrique Actions, ressources et clés de condition pour AWS Lambda dans la Référence de l'autorisation de service.

Rubriques

- Bonnes pratiques en matière de politiques
- Utilisation de la console Lambda
- Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Bonnes pratiques en matière de politiques

Identity-based les politiques déterminent si quelqu'un peut créer, accéder ou supprimer des ressources Lambda dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.
- Accordez les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation d'IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utilisez des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez l'Analyseur d'accès IAM pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : l'Analyseur d'accès IAM valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez Validation de politiques avec IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger la MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Sécurisation de l'accès aux API avec MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Utilisation de la console Lambda

Pour accéder à la AWS Lambda console, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et d'afficher des informations détaillées sur les ressources Lambda de votre. Compte AWS Si vous créez une politique basée sur l'identité qui est plus restrictive que l'ensemble minimum d'autorisations requis, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) tributaires de cette politique.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API qu'ils tentent d'effectuer.

Pour obtenir un exemple de stratégie qui accorde un accès minimal pour le développement de fonctions, veuillez consulter Autoriser les utilisateurs à accéder à une fonction événementielle. En plus des API Lambda, la console Lambda utilise d'autres services pour afficher la configuration des déclencheurs et vous permettre d'en ajouter de nouveaux. Si vos utilisateurs utilisent Lambda avec d'autres services, ils ont également besoin d'accéder à ces services. Pour plus d'informations sur la configuration d'autres services avec Lambda, consultez Invoquer Lambda avec des événements provenant d'autres AWS services.

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d'afficher les politiques en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide de l'API AWS CLI or AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
```

```
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS politiques gérées pour AWS Lambda

Une politique AWS gérée est une politique autonome créée et administrée par AWS. AWS les politiques gérées sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

N'oubliez pas que les politiques AWS gérées peuvent ne pas accorder d'autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont accessibles à tous les AWS clients. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client qui sont propres à vos cas d’utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées. Si les autorisations définies dans une politique AWS gérée sont AWS mises à jour, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée. AWS est le plus susceptible de mettre à jour une politique AWS gérée lorsqu'une nouvelle politique Service AWS est lancée ou lorsque de nouvelles opérations d'API sont disponibles pour les services existants.

Pour plus d'informations, consultez Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

Rubriques

- AWS politique gérée : AWS Lambda_FullAccess
- AWS politique gérée : AWS Lambda_ReadOnlyAccess
- AWS politique gérée : AWSLambdaBasicExecutionRole
- AWS politique gérée : AWSLambdaBasicDurableExecutionRolePolicy
- AWS politique gérée : AWSLambdaDynamoDBExecutionRole
- AWS politique gérée : AWSLambdaENIManagementAccess
- AWS politique gérée : AWSLambdaInvocation-DynamoDB
- AWS politique gérée : AWSLambdaKinesisExecutionRole
- AWS politique gérée : AWSLambdaMSKExecutionRole
- AWS politique gérée : AWSLambdaRole
- AWS politique gérée : AWSLambdaSQSQueueExecutionRole
- AWS politique gérée : AWSLambdaVPCAccessExecutionRole
- AWS politique gérée : AWSLambdaManagedEC2ResourceOperator
- AWS politique gérée : AWSLambdaServiceRolePolicy
- AWS politique gérée : AWSLambdaNetworkConnectorOperatorPolicy
- AWS politique gérée : AWSLambdaInvokeWebFunctionEndpointAccess
- Lambda met à jour ses AWS stratégies gérées

AWS politique gérée : AWS Lambda_FullAccess

Cette stratégie accorde un accès complet aux actions Lambda. Il accorde également des autorisations à d'autres AWS services utilisés pour développer et gérer les ressources Lambda.

Vous pouvez attacher la stratégie `AWSLambda_FullAccess` à vos utilisateurs, groupes et rôles.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

- `lambda` : donne aux principaux un accès complet à Lambda.

- `cloudformation`— Permet aux directeurs de décrire les AWS CloudFormation piles et de répertorier les ressources qu'elles contiennent.
- `cloudwatch`— Permet aux principaux de répertorier les CloudWatch métriques Amazon et d'obtenir des données métriques.
- `ec2` : permet aux principaux de décrire les groupes de sécurité, les sous-réseaux et les VPC.
- `iam` : permet aux principaux d'obtenir les stratégies, les versions des stratégies, les rôles, les stratégies de rôle, les stratégies de rôles associées et la liste des rôles. Cette stratégie permet également aux principaux de transmettre des rôles à Lambda. L'autorisation `PassRole` est utilisée lorsque vous attribuez un rôle d'exécution à une fonction. L'`CreateServiceLinkedRole`autorisation est utilisée lors de la création d'un rôle lié à un service.
- `kms`— Permet aux principaux de répertorier les alias et de décrire la clé pour le chiffrement des volumes.
- `logs` : permet aux principaux de décrire les flux de journaux, d'obtenir les événements du journal, de filtrer les événements du journal et de démarrer et arrêter dsessions Live Tail.
- `states`— Permet aux directeurs de décrire et de répertorier les machines AWS Step Functions d'état.
- `tag` : permet aux principaux d'obtenir des ressources en fonction de leurs balises.
- `xray`— Permet aux principaux d'obtenir des résumés de AWS X-Ray traces et de récupérer une liste de traces spécifiée par ID.

Pour plus d'informations sur cette politique, y compris le document de politique JSON et les versions de politique, consultez AWS Lambda_FullAccess dans le AWS Managed Policy Reference Guide.

AWS politique gérée : AWS Lambda_ReadOnlyAccess

Cette politique accorde un accès en lecture seule aux ressources Lambda et aux autres AWS services utilisés pour développer et gérer les ressources Lambda.

Vous pouvez attacher la stratégie `AWSLambda_ReadOnlyAccess` à vos utilisateurs, groupes et rôles.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

- `lambda` : permet aux principaux d'obtenir et de répertorier toutes les ressources.
- `cloudformation`— Permet aux directeurs de décrire et de répertorier les AWS CloudFormation piles et de répertorier les ressources qu'elles contiennent.
- `cloudwatch`— Permet aux principaux de répertorier les CloudWatch métriques Amazon et d'obtenir des données métriques.
- `ec2` : permet aux principaux de décrire les groupes de sécurité, les sous-réseaux et les VPC.
- `iam` : permet aux principaux d'obtenir les stratégies, les versions des stratégies, les rôles, les stratégies de rôle, les stratégies de rôles associées et la liste des rôles.
- `kms` : permet aux principaux de répertorier les alias.
- `logs` : permet aux principaux de décrire les flux de journaux, d'obtenir les événements du journal, de filtrer les événements du journal et de démarrer et arrêter dsessions Live Tail.
- `states`— Permet aux directeurs de décrire et de répertorier les machines AWS Step Functions d'état.
- `tag` : permet aux principaux d'obtenir des ressources en fonction de leurs balises.
- `xray`— Permet aux principaux d'obtenir des résumés de AWS X-Ray traces et de récupérer une liste de traces spécifiée par ID.

Pour plus d'informations sur cette politique, y compris le document de politique JSON et les versions de politique, consultez AWS Lambda_ReadOnlyAccess dans le AWS Managed Policy Reference Guide.

AWS politique gérée : AWSLambdaBasicExecutionRole

Cette politique accorde des autorisations pour télécharger des CloudWatch journaux dans Logs.

Vous pouvez attacher la stratégie `AWSLambdaBasicExecutionRole` à vos utilisateurs, groupes et rôles.

Pour plus d'informations sur cette politique, y compris le document de politique JSON et les versions de politique, consultez AWSLambdaBasicExecutionRolele Guide de référence des politiques AWS gérées.

AWS politique gérée : AWSLambdaBasicDurableExecutionRolePolicy

Cette politique fournit des autorisations d'écriture aux CloudWatch journaux et des read/write autorisations aux API d'exécution durable utilisées par les fonctions durables Lambda. Cette politique

fournit les autorisations essentielles requises pour les fonctions durables Lambda, qui utilisent des API d'exécution durables pour maintenir la progression et maintenir l'état d'un appel de fonction à l'autre.

Vous pouvez attacher la stratégie `AWSLambdaBasicDurableExecutionRolePolicy` à vos utilisateurs, groupes et rôles.

Détails de l’autorisation

Cette politique inclut les autorisations suivantes :

- `logs`— Permet aux principaux de créer des groupes de journaux et des flux de journaux, et d'écrire les événements des journaux dans les CloudWatch journaux.
- `lambda`— Permet aux principaux de vérifier l'état d'exécution durable et de récupérer l'état d'exécution durable pour les fonctions durables Lambda.

Pour plus de détails sur cette politique, y compris la dernière version du document sur la politique JSON, consultez AWSLambdaBasicDurableExecutionRolePolicy dans le Guide de référence de la politique gérée par AWS .

AWS politique gérée : AWSLambdaDynamoDBExecutionRole

Cette politique accorde des autorisations pour lire les enregistrements d'un flux Amazon DynamoDB et pour écrire dans Logs. CloudWatch

Vous pouvez attacher la stratégie `AWSLambdaDynamoDBExecutionRole` à vos utilisateurs, groupes et rôles.

Pour plus d'informations sur cette politique, y compris le document de politique JSON et les versions de politique, consultez AWSLambdaDynamoDBExecutionRolele Guide de référence des politiques AWS gérées.

AWS politique gérée : AWSLambdaENIManagementAccess

Cette politique accorde des autorisations pour créer, décrire et supprimer des interfaces réseau élastiques utilisées par une fonction VPC-enabled Lambda.

Vous pouvez attacher la stratégie `AWSLambdaENIManagementAccess` à vos utilisateurs, groupes et rôles.

Pour plus d'informations sur cette politique, y compris le document de politique JSON et les versions de politique, consultez AWSLambdaENIManagementAccessle Guide de référence des politiques AWS gérées.

AWS politique gérée : AWSLambdaInvocation-DynamoDB

Cette stratégie accorde un accès en lecture à Amazon DynamoDB Streams.

Vous pouvez attacher la stratégie `AWSLambdaInvocation-DynamoDB` à vos utilisateurs, groupes et rôles.

Pour plus d'informations sur cette politique, y compris le document de politique JSON et les versions de politique, consultez AWSLambdaInvocation-DynamoDBle Guide de référence des politiques AWS gérées.

AWS politique gérée : AWSLambdaKinesisExecutionRole

Cette politique accorde l'autorisation de lire les événements d'un flux de données Amazon Kinesis et d'écrire dans Logs. CloudWatch

Vous pouvez attacher la stratégie `AWSLambdaKinesisExecutionRole` à vos utilisateurs, groupes et rôles.

Pour plus d'informations sur cette politique, y compris le document de politique JSON et les versions de politique, consultez AWSLambdaKinesisExecutionRolele Guide de référence des politiques AWS gérées.

AWS politique gérée : AWSLambdaMSKExecutionRole

Cette politique autorise la lecture et l'accès aux enregistrements d'un cluster Amazon Managed Streaming for Apache Kafka, la gestion des interfaces réseau élastiques et l'écriture dans les CloudWatch journaux.

Vous pouvez attacher la stratégie `AWSLambdaMSKExecutionRole` à vos utilisateurs, groupes et rôles.

Pour plus d'informations sur cette politique, y compris le document de politique JSON et les versions de politique, consultez AWSLambdaMSKExecutionRolele Guide de référence des politiques AWS gérées.

AWS politique gérée : AWSLambdaRole

Cette stratégie accorde des autorisations pour invoquer les fonctions Lambda.

Vous pouvez attacher la stratégie `AWSLambdaRole` à vos utilisateurs, groupes et rôles.

Pour plus d'informations sur cette politique, y compris le document de politique JSON et les versions de politique, consultez AWSLambdaRolele Guide de référence des politiques AWS gérées.

AWS politique gérée : AWSLambdaSQSQueueExecutionRole

Cette politique accorde des autorisations pour lire et supprimer des messages d'une file d'attente Amazon Simple Queue Service, et accorde des autorisations d'écriture aux CloudWatch journaux.

Vous pouvez attacher la stratégie `AWSLambdaSQSQueueExecutionRole` à vos utilisateurs, groupes et rôles.

Pour plus d'informations sur cette politique, y compris le document de politique JSON et les versions de politique, consultez AWSLambdaSQSQueueExecutionRolele Guide de référence des politiques AWS gérées.

AWS politique gérée : AWSLambdaVPCAccessExecutionRole

Cette politique accorde des autorisations pour gérer des interfaces réseau élastiques au sein d'un Amazon Virtual Private Cloud et pour écrire dans CloudWatch Logs.

Vous pouvez attacher la stratégie `AWSLambdaVPCAccessExecutionRole` à vos utilisateurs, groupes et rôles.

Pour plus d'informations sur cette politique, y compris le document de politique JSON et les versions de politique, consultez AWSLambdaVPCAccessExecutionRolele Guide de référence des politiques AWS gérées.

AWS politique gérée : AWSLambdaManagedEC2ResourceOperator

Cette politique permet la gestion automatisée des instances Amazon Elastic Compute Cloud et la CloudWatch journalisation Amazon pour les fournisseurs de capacité Lambda. Il autorise Lambda à effectuer des opérations sur le cycle de vie des instances et à écrire des journaux en votre nom.

Vous pouvez attacher la stratégie `AWSLambdaManagedEC2ResourceOperator` à vos utilisateurs, groupes et rôles.

Détails de l’autorisation

Cette politique inclut les autorisations suivantes :

- `ec2:RunInstances`— Permet à Lambda de lancer de nouvelles instances Amazon EC2 à condition que ec2 ManagedResourceOperator : soit égal à scaler.lambda.amazonaws.com et limite l'utilisation des AMI aux images uniquement. Amazon-owned
- `ec2:DescribeInstances`et `ec2:DescribeInstanceStatus` — Permet à Lambda de surveiller l'état de l'instance et de récupérer les informations relatives à l'instance.
- `ec2:CreateTags`— Permet à Lambda de baliser les ressources Amazon EC2 à des fins de gestion et d'identification.
- `ec2:DescribeAvailabilityZones`— Permet à Lambda de visualiser les zones disponibles pour les décisions de placement des instances.
- `ec2:DescribeCapacityReservations`— Permet à Lambda de vérifier les réservations de capacité pour un placement optimal des instances.
- `ec2:DescribeInstanceTypes`et `ec2:DescribeInstanceTypeOfferings` — Permet à Lambda de passer en revue les types d'instances disponibles et leurs offres.
- `ec2:DescribeSubnets`— Permet à Lambda d'examiner les configurations de sous-réseau pour la planification du réseau.
- `ec2:DescribeVpcEncryptionControls`— Permet à Lambda d'examiner les paramètres de contrôle du chiffrement VPC pour la configuration de l'instance.
- `ec2:DescribeSecurityGroups`— Permet à Lambda de récupérer les informations du groupe de sécurité pour la configuration de l'interface réseau.
- `ec2:CreateNetworkInterface`— Permet à Lambda de créer des interfaces réseau et de gérer les associations de sous-réseaux et de groupes de sécurité.
- `ec2:AttachNetworkInterface`— Permet à Lambda d'associer des interfaces réseau aux instances Amazon EC2 avec la condition `ec2:ManagedResourceOperator` égale à scaler.lambda.amazonaws.com.
- `logs:CreateLogGroup`— Permet à Lambda de créer des groupes de journaux de CloudWatch journaux.
- `logs:CreateLogStream`et `logs:PutLogEvents` — Permet à Lambda de créer des flux de journaux et d'écrire des événements de journal dans des journaux. CloudWatch

Pour plus d'informations sur cette politique, y compris le document de politique JSON et les versions de politique, consultez AWSLambdaManagedEC2ResourceOperatorle Guide de référence des politiques AWS gérées.

AWS politique gérée : AWSLambdaServiceRolePolicy

Cette politique est attachée au rôle lié au service nommé pour permettre AWSServiceRoleForLambda à Lambda de 1) mettre fin aux instances gérées dans le cadre des fournisseurs de capacité Lambda et 2) de supprimer les interfaces réseau Elastic (ENI) gérées dans le cadre des connecteurs réseau Lambda.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

- `ec2:TerminateInstances`— Permet à Lambda de mettre fin aux instances EC2 à la condition que ec2 : soit égal à scaler.lambda.amazonaws.com. ManagedResourceOperator
- `ec2:DescribeInstanceStatus`et `ec2:DescribeInstances` — Permet à Lambda de décrire les instances EC2.
- `ec2:DescribeNetworkInterfaces`,`ec2:DescribeSubnets`, et `ec2:DescribeSecurityGroups` — Permet à Lambda de décrire les interfaces réseau, les sous-réseaux et les groupes de sécurité.
- `ec2:DeleteNetworkInterface`— Permet à Lambda de supprimer les ENI à condition que ec2 : soit égal à network-connectors.lambda.amazonaws.com. ManagedResourceOperator

Pour plus d'informations sur cette politique, consultez la section Utilisation de rôles liés à un service pour Lambda.

AWS politique gérée : AWSLambdaNetworkConnectorOperatorPolicy

Cette politique accorde des autorisations pour créer et administrer des ressources Elastic Network Interface (ENI) gérées par le Lambda Network Connector.

Vous pouvez attacher la stratégie `AWSLambdaNetworkConnectorOperatorPolicy` à vos utilisateurs, groupes et rôles.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

- `ec2:CreateNetworkInterface`— Accorde l'autorisation de créer des interfaces réseau dans n'importe quel sous-réseau avec des groupes de sécurité associés. Pour les ressources de l'interface réseau, seules les balises contenant `aws:lambda:networkConnectorName` les clés `aws:lambda:networkConnectorId` sont autorisées.

- `ec2:CreateTags`— Accorde l'autorisation de baliser les interfaces réseau au moment de leur création. Cette autorisation s'applique uniquement lorsque l'action de création est effectuée `CreateNetworkInterface` et que l'opérateur de ressources gérées l'est`network-connectors.lambda.amazonaws.com`.

Pour plus d'informations sur cette politique, y compris le document de politique JSON et les versions de politique, consultez AWSLambdaNetworkConnectorOperatorPolicyle Guide de référence des politiques AWS gérées.

AWS politique gérée : AWSLambdaInvokeWebFunctionEndpointAccess

Cette politique accorde l'autorisation d'invoquer les points de terminaison des fonctions Web Lambda.

Vous pouvez attacher la stratégie `AWSLambdaInvokeWebFunctionEndpointAccess` à vos utilisateurs, groupes et rôles.

Pour plus d'informations sur cette politique, y compris le document de politique JSON et les versions de politique, consultez AWSLambdaInvokeWebFunctionEndpointAccessle Guide de référence des politiques AWS gérées.

Lambda met à jour ses AWS stratégies gérées

Modifier	Description	Date
AWSLambdaInvokeWebFunctionEndpointAccess : nouvelle politique	Lambda a ajouté une nouvelle politique gérée pour accorder des autorisations permettant d'invoquer les points de terminaison des fonctions Web Lambda.	1 octobre 2026
AWSLambdaNetworkConnectorOperatorPolicy : nouvelle politique	Lambda a ajouté une nouvelle politique gérée pour accorder des autorisations pour créer et administrer des ressources ENI gérées par le connecteur réseau Lambda.	19 juin 2026

Modifier	Description	Date
AWSLambdaManagedEC2ResourceOperator— Modification	Lambda a mis à jour la `AWSLambdaManagedEC2ResourceOperator` politique pour autoriser les `logs:CreateLogGroup` actions `logs:CreateLogStream` , et `logs:PutLogEvents` . Ces autorisations permettent à Lambda d'écrire des journaux dans Logs. CloudWatch	10 juin 2026
AWSLambdaManagedEC2ResourceOperator— Modification	Lambda a mis à jour la `AWSLambdaManagedEC2ResourceOperator` politique pour autoriser l'`ec2:DescribeVpcEncryptionControls` action. Cette autorisation permet à Lambda d'examiner les paramètres de contrôle du chiffrement VPC pour la configuration de l'instance.	23 avril 2026
AWSLambdaManagedEC2ResourceOperator : nouvelle politique	Lambda a ajouté une nouvelle politique gérée pour permettre la gestion automatisée des instances Amazon EC2 pour les fournisseurs de capacité Lambda, permettant ainsi au service de scaler d'effectuer des opérations sur le cycle de vie des instances.	30 novembre 2025

Modifier	Description	Date
AWSLambdaServiceRolePolicy : nouvelle politique	Lambda a ajouté une nouvelle politique gérée pour le rôle lié au service afin de permettre à Lambda de mettre fin aux instances gérées dans le cadre des fournisseurs de capacité Lambda.	30 novembre 2025
AWS Lambda_FullAccess — Modification	Lambda a mis à jour la `AWSLambda_FullAccess` politique pour autoriser les actions `kms:DescribeKey` et `iam:CreateServiceLinkedRole` .	30 novembre 2025
AWSLambdaBasicDurableExecutionRolePolicy— Nouvelle politique gérée	Lambda a publié une nouvelle politique gérée `AWSLambdaBasicDurableExecutionRolePolicy` qui fournit des autorisations d'écriture aux CloudWatch journaux et des read/write autorisations aux API d'exécution durable utilisées par les fonctions durables Lambda.	1er décembre 2025
AWS Lambda_ReadOnlyAccess et AWS Lambda_FullAccess — Modification	Lambda a mis à jour les politiques `AWSLambda_ReadOnlyAccess` et `AWSLambda_FullAccess` pour autoriser les actions `logs:StartLiveTail` et `logs:StopLiveTail` .	17 mars 2025

Modifier	Description	Date
AWSLambdaVPCAccessExecutionRole— Modification	Lambda a mis à jour la politique `AWSLambdaVPCAccessExecutionRole` pour autoriser l'action `ec2:DescribeSubnets` .	5 janvier 2024
AWS Lambda_ReadOnlyAccess — Modification	Lambda a mis à jour la `AWSLambda_ReadOnlyAccess` politique pour autoriser les principaux à répertorier les piles. CloudFormation	27 juillet 2023
AWS Lambda a commencé à suivre les modifications	AWS Lambda a commencé à suivre les modifications apportées AWS à ses politiques gérées.	27 juillet 2023

Résolution des problèmes AWS Lambda identité et accès

Utilisez les informations suivantes pour identifier et résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec Lambda et IAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action dans Lambda
- Je ne suis pas autorisé à effectuer iam : PassRole
- Je souhaite autoriser des personnes extérieures à mon Compte AWS pour accéder à mes ressources Lambda

Je ne suis pas autorisé à effectuer une action dans Lambda

Si vous recevez une erreur qui indique que vous n'êtes pas autorisé à effectuer une action, vos politiques doivent être mises à jour afin de vous permettre d'effectuer l'action.

L'exemple d'erreur suivant se produit quand l'utilisateur IAM `mateojackson` tente d'utiliser la console pour afficher des informations détaillées sur une ressource *`my-example-widget`* fictive, mais ne dispose pas des autorisations `lambda:`*`GetWidget`* fictives.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 lambda:GetWidget on resource: my-example-widget
```

Dans ce cas, la politique qui s'applique à l'utilisateur `mateojackson` doit être mise à jour pour autoriser l'accès à la ressource *`my-example-widget`* à l'aide de l'action `lambda:`*`GetWidget`*.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez une erreur selon laquelle vous n'êtes pas autorisé à exécuter l'action `iam:PassRole`, vos politiques doivent être mises à jour pour vous permettre de transmettre un rôle à Lambda.

Certains vous Services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, vous devez disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit quand un utilisateur IAM nommé `marymajor` tente d'utiliser la console pour exécuter une action dans Lambda. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary n'est pas autorisée à transmettre le rôle au service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite autoriser des personnes extérieures à mon Compte AWS pour accéder à mes ressources Lambda

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACL), vous pouvez utiliser ces politiques pour donner l'accès à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si Lambda prend en charge ces fonctions, consultez Comment ? AWS Lambda fonctionne avec IAM.
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.
- Pour en savoir plus sur la différence entre l'utilisation des rôles et des politiques basées sur les ressources pour l'accès intercompte, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Création d'une stratégie de gouvernance pour les couches et les fonctions Lambda

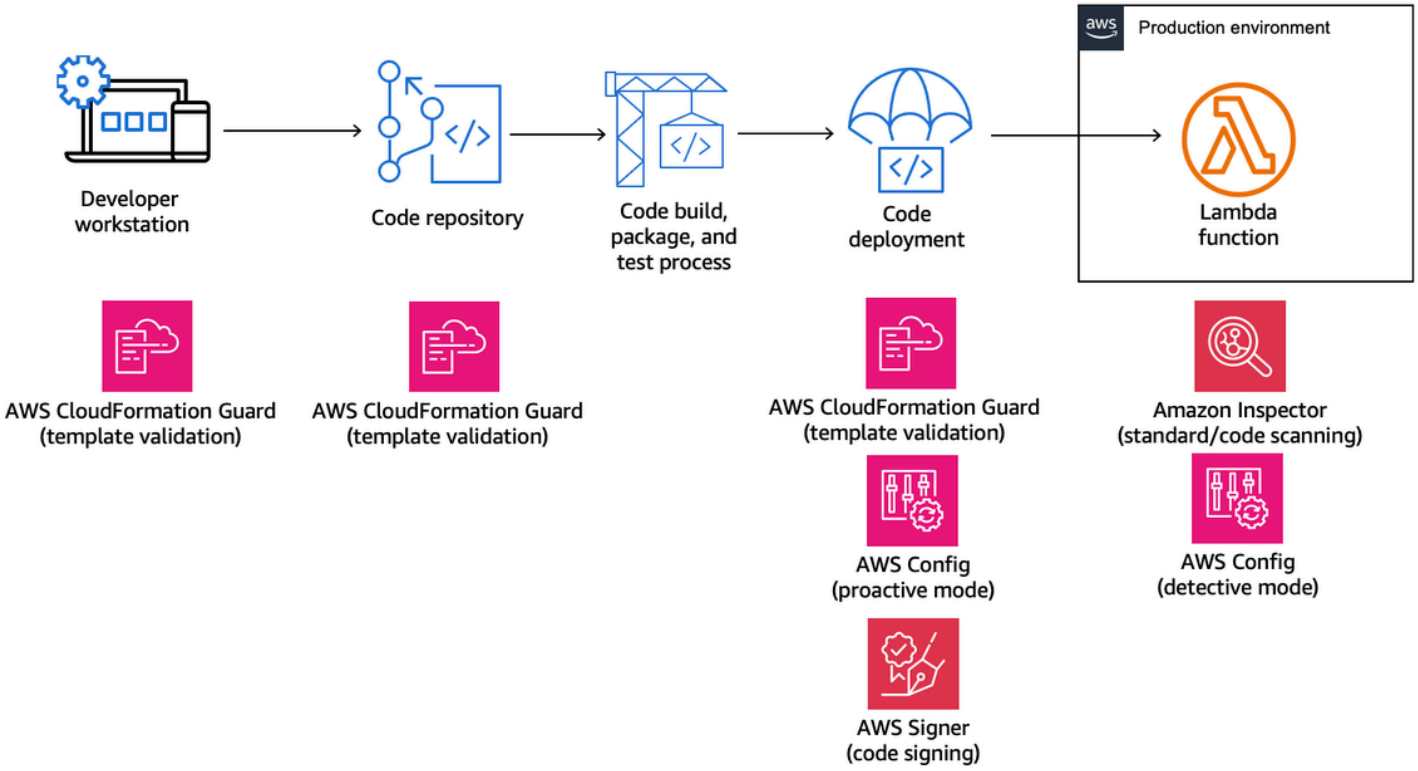
Pour créer et déployer des applications cloud natives sans serveur, vous devez garantir agilité et rapidité de mise sur le marché grâce à une gouvernance et à des barrières de protection appropriés. Vous définissez des priorités au niveau de l'entreprise, en mettant peut-être l'accent sur l'agilité comme priorité absolue, ou en mettant l'accent sur l'aversion au risque par le biais de la gouvernance, des garde-fous et des contrôles. En réalité, vous n'aurez pas de stratégie « » mais une stratégie either/or « et » qui équilibre à la fois agilité et garde-fous dans le cycle de vie de votre

développement logiciel. Quelle que soit la place de ces exigences dans le cycle de vie de votre entreprise, les capacités de gouvernance sont susceptibles de devenir une exigence de mise en œuvre dans vos processus et chaînes d'outils.

Voici quelques exemples de contrôles de gouvernance qu'une organisation peut mettre en œuvre pour Lambda :

- Les fonctions Lambda ne doivent pas être publiquement accessibles.
- Les fonctions Lambda doivent être associées à un VPC.
- Les fonctions Lambda ne doivent pas utiliser d'environnements d'exécution obsolètes.
- Les fonctions Lambda doivent être étiquetées avec un ensemble de balises obligatoires.
- Les couches Lambda ne doivent pas être accessibles en dehors de l'organisation.
- Les fonctions Lambda associées à un groupe de sécurité doivent avoir des balises correspondantes entre la fonction et le groupe de sécurité.
- Les fonctions Lambda associées à une couche doivent utiliser une version approuvée
- Les variables d'environnement Lambda doivent être chiffrées au repos avec une clé gérée par le client.

Le schéma suivant est un exemple de stratégie de gouvernance approfondie qui met en œuvre des contrôles et des politiques tout au long du processus de développement et de déploiement du logiciel :



Les rubriques suivantes expliquent comment implémenter des contrôles pour développer et déployer des fonctions Lambda dans votre organisation, à la fois pour la start-up et pour l'entreprise. Votre organisation possède peut-être déjà des outils en place. Les rubriques suivantes adoptent une approche modulaire de ces contrôles, afin que vous puissiez sélectionner les composants dont vous avez réellement besoin. Les sujets incluent the section called “Contrôles proactifs avec Guard”the section called “Analyse du code”,the section called “Signature de code”, etthe section called “Observabilité”.

Rubriques

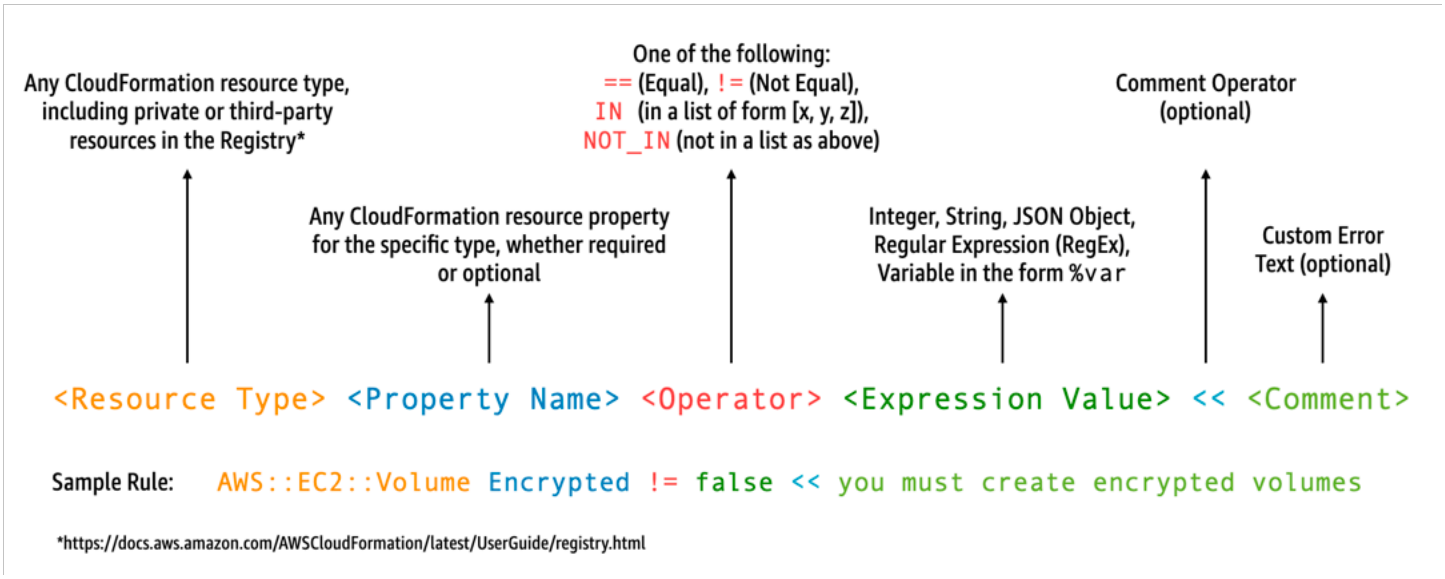
- Contrôles proactifs pour Lambda avec AWS CloudFormation Guard
- Mettez en œuvre des contrôles préventifs pour Lambda avec AWS Config
- Détectez les déploiements et les configurations Lambda non conformes avec AWS Config
- Signature de code Lambda avec AWS Signer
- Automatisation des évaluations de sécurité pour Lambda avec Amazon Inspector
- Mettre en œuvre l'observabilité pour la sécurité et la conformité Lambda

Contrôles proactifs pour Lambda avec AWS CloudFormation Guard

AWS CloudFormation Guard est un outil d'évaluation des politiques en tant que code open source à usage général. Cela peut être utilisé à des fins de gouvernance préventive et de conformité en validant les modèles d'infrastructure en tant que code (IaC) et les compositions de services par rapport aux règles de politique. Ces règles peuvent être personnalisées en fonction des exigences de votre équipe ou de votre organisation. Pour les fonctions Lambda, les règles Guard peuvent être utilisées pour contrôler la création de ressources et les mises à jour de configuration en définissant les paramètres de propriété requis lors de la création ou de la mise à jour d'une fonction Lambda.

Les administrateurs de conformité définissent la liste des contrôles et des politiques de gouvernance nécessaires au déploiement et à la mise à jour des fonctions Lambda. Les administrateurs de la plateforme implémentent les contrôles dans les CI/CD pipelines, sous forme de webhooks de validation avant validation avec des référentiels de code, et fournissent aux développeurs des outils de ligne de commande pour valider les modèles et le code sur les postes de travail locaux. Les développeurs créent du code, valident des modèles à l'aide d'outils de ligne de commande, puis valident le code dans des référentiels, qui sont ensuite automatiquement validés via les CI/CD pipelines avant le déploiement dans un AWS environnement.

Avec Guard, vous pouvez écrire vos règles et implémenter vos contrôles dans un langage spécifique au domaine comme suit.



Supposons, par exemple, que vous souhaitiez vous assurer que les développeurs choisissent uniquement les derniers environnements d'exécution. Vous pouvez spécifier deux politiques différentes, l'une pour identifier les environnements d'exécution déjà obsolètes et l'autre pour

identifier les environnements d'exécution qui le seront bientôt. Pour cela, vous pouvez écrire le fichier `etc/rules.guard` suivant :

```
let lambda_functions = Resources.*[
    Type == "AWS::Lambda::Function"
]

rule lambda_already_deprecated_runtime when %lambda_functions !empty {
    %lambda_functions {
        Properties {
            when Runtime exists {
                Runtime !in ["dotnetcore3.1", "nodejs12.x", "python3.6", "python2.7",
 "dotnet5.0", "dotnetcore2.1", "ruby2.5", "nodejs10.x", "nodejs8.10", "nodejs4.3",
 "nodejs6.10", "dotnetcore1.0", "dotnetcore2.0", "nodejs4.3-edge", "nodejs"] <<Lambda
 function is using a deprecated runtime.>>
            }
        }
    }
}

rule lambda_soon_to_be_deprecated_runtime when %lambda_functions !empty {
    %lambda_functions {
        Properties {
            when Runtime exists {
                Runtime !in ["nodejs16.x", "nodejs14.x", "python3.7", "java8",
 "dotnet7", "go1.x", "ruby2.7", "provided"] <<Lambda function is using a runtime that
 is targeted for deprecation.>>
            }
        }
    }
}
```

Supposons maintenant que vous écriviez le `iac/lambda.yaml` CloudFormation modèle suivant qui définit une fonction Lambda :

```
  Fn:
    Type: AWS::Lambda::Function
    Properties:
      Runtime: python3.7
      CodeUri: src
      Handler: fn.handler
      Role: !GetAtt FnRole.Arn
      Layers:
```

```
        - arn:aws:lambda:us-east-1:111122223333:layer:LambdaInsightsExtension:35
```

Après avoir installé l'utilitaire Guard, validez votre modèle :

```
cfn-guard validate --rules etc/rules.guard --data iac/lambda.yaml
```

Le résultat se présente comme suit :

```
lambda.yaml Status = FAIL
FAILED rules
rules.guard/lambda_soon_to_be_deprecated_runtime
---
Evaluating data lambda.yaml against rules rules.guard
Number of non-compliant resources 1
Resource = Fn {
  Type      = AWS::Lambda::Function
  Rule = lambda_soon_to_be_deprecated_runtime {
    ALL {
      Check =  Runtime not IN
 ["nodejs16.x","nodejs14.x","python3.7","java8","dotnet7","go1.x","ruby2.7","provided"]
 {
       ComparisonError {
         Message          = Lambda function is using a runtime that is targeted for
 deprecation.
         Error            = Check was not compliant as property [/Resources/
Fn/Properties/Runtime[L:88,C:15]] was not present in [(resolved, Path=[L:0,C:0]
 Value=["nodejs16.x","nodejs14.x","python3.7","java8","dotnet7","go1.x","ruby2.7","provided"])]
       }
         PropertyPath    = /Resources/Fn/Properties/Runtime[L:88,C:15]
         Operator        = NOT IN
         Value           = "python3.7"
         ComparedWith    =
 [["nodejs16.x","nodejs14.x","python3.7","java8","dotnet7","go1.x","ruby2.7","provided"]]
         Code:
              86.  Fn:
              87.    Type: AWS::Lambda::Function
              88.    Properties:
              89.      Runtime: python3.7
              90.      CodeUri: src
              91.      Handler: fn.handler

      }
    }
```

```
  }
}
```

Avec Guard, vos développeurs peuvent voir depuis leur poste de travail local qu'ils ont besoin de mettre à jour le modèle pour utiliser un environnement d'exécution autorisé par l'organisation. Cela se produit avant de valider dans un référentiel de code et d'échouer ensuite aux vérifications au sein d'un CI/CD pipeline. Vos développeurs reçoivent ainsi des informations sur la manière de développer des modèles conformes et de consacrer leur temps à l'écriture de code apportant une valeur commerciale. Ce contrôle peut être appliqué sur la station de travail du développeur local, dans un webhook de validation préalable à la validation, and/or dans le CI/CD pipeline avant le déploiement.

Mises en garde

Si vous utilisez des modèles AWS Serverless Application Model (AWS SAM) pour définir des fonctions Lambda, sachez que vous devez mettre à jour la règle Guard pour rechercher le type de `AWS::Serverless::Function` ressource comme suit.

```
let lambda_functions = Resources.*[
    Type == "AWS::Serverless::Function"
]
```

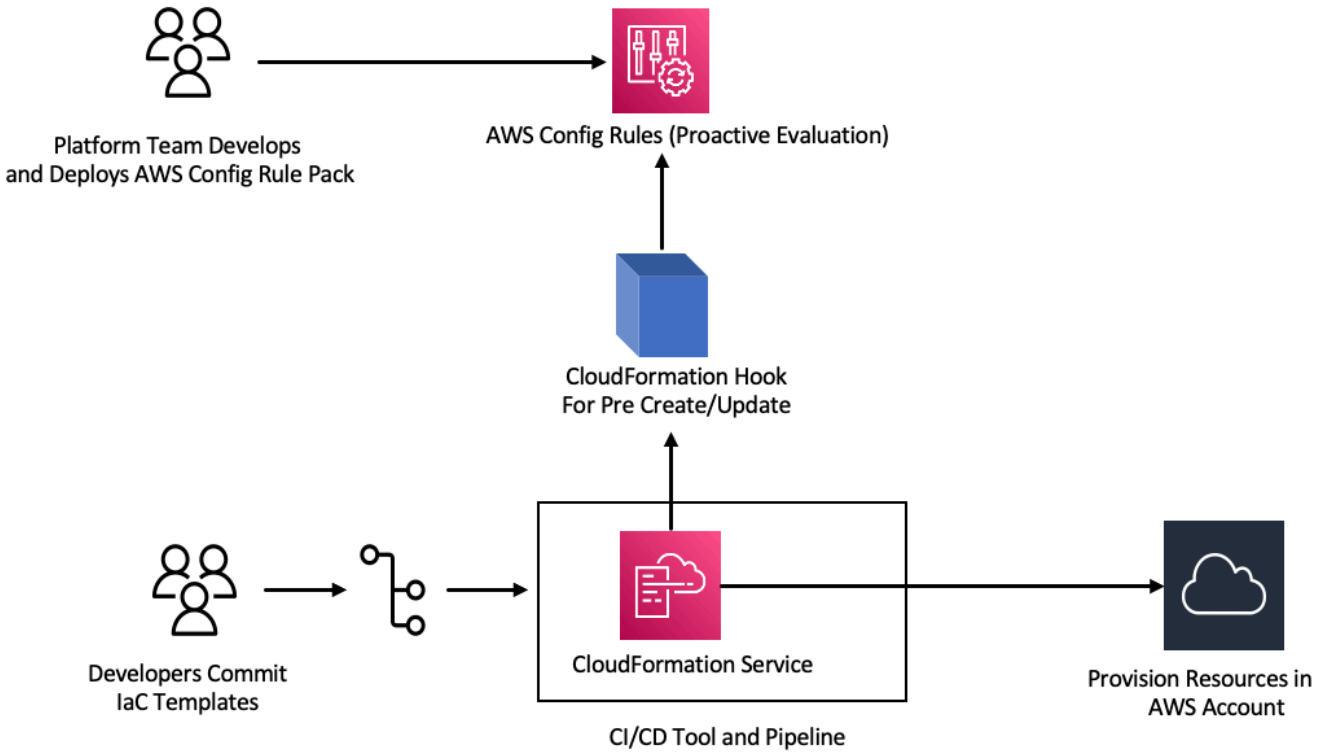
Guard s'attend également à ce que les propriétés soient incluses dans la définition de la ressource. Dans le même temps, les AWS SAM modèles permettent de spécifier les propriétés dans une section Globals distincte. Les propriétés définies dans la section Globals ne sont pas validées par vos règles Guard.

Comme indiqué dans la documentation de dépannage de Guard, sachez que Guard ne prend pas en charge les formulaires intrinsèques abrégés tels que `!GetAtt` ou `!Sub` et nécessite plutôt l'utilisation des formulaires étendus : `Fn::GetAtt` et. `Fn::Sub` (L'exemple précédent n'évaluant pas la propriété Role, la forme abrégée intrinsèque a été utilisée pour des raisons de simplicité.)

Mettez en œuvre des contrôles préventifs pour Lambda avec AWS Config

Il est essentiel de garantir la conformité de vos applications sans serveur le plus tôt possible dans le processus de développement. Dans cette rubrique, nous expliquons comment mettre en œuvre des contrôles préventifs à l'aide de AWS Config. Grâce à AWS Config, vous pouvez mettre en œuvre des contrôles de conformité plus tôt dans le processus de développement et implémenter les mêmes contrôles dans vos CI/CD pipelines. Cela permet également de normaliser vos contrôles dans un référentiel de règles géré de manière centralisée afin que vous puissiez appliquer vos contrôles de manière cohérente à tous vos AWS comptes.

Supposons, par exemple, que vos administrateurs de conformité aient défini une exigence garantissant que toutes les fonctions Lambda incluent le AWS X-Ray traçage. Grâce AWS Config au mode proactif, vous pouvez effectuer des contrôles de conformité sur les ressources de vos fonctions Lambda avant le déploiement, réduisant ainsi le risque de déploiement de fonctions Lambda mal configurées et faisant gagner du temps aux développeurs en leur fournissant des informations plus rapides sur l'infrastructure sous forme de modèles de code. Voici une visualisation du flux pour les contrôles préventifs avec AWS Config :



Envisagez d'exiger que le suivi soit activé pour toutes les fonctions Lambda. En réponse, l'équipe de la plateforme identifie la nécessité d'une AWS Config règle spécifique à exécuter de manière proactive sur tous les comptes. Cette règle signale toute fonction Lambda qui ne dispose pas d'une configuration de X-Ray suivi configurée comme une ressource non conforme. L'équipe développe une règle, la regroupe dans un pack de conformité et déploie le pack de conformité sur tous les comptes afin de s'assurer que tous les AWS comptes de l'organisation appliquent ces contrôles de manière uniforme. Vous pouvez écrire la règle dans la syntaxe AWS CloudFormation Guard 2.x.x, qui prend la forme suivante :

```
rule name when condition { assertion }
```

Voici un exemple de règle Guard qui vérifie que le suivi est activé pour les fonctions Lambda :

```
rule lambda_tracing_check {
  when configuration.tracingConfig exists {
      configuration.tracingConfig.mode == "Active"
  }
}
```

L'équipe de la plateforme prend des mesures supplémentaires en exigeant que chaque AWS CloudFormation déploiement invoque un create/update pré-hook. Elle assume l'entière responsabilité du développement de ce hook et de la configuration du pipeline, du renforcement du contrôle centralisé des règles de conformité et du maintien de leur application cohérente dans tous les déploiements. Pour développer, empaqueter et enregistrer un hook, consultez la section Développement de AWS CloudFormation hooks dans la documentation de l'interface de ligne de CloudFormation commande (CFN-CLI). Vous pouvez utiliser la CloudFormation CLI pour créer le projet hook :

```
cfn init
```

Cette commande vous demande des informations de base sur votre projet hook et crée un projet contenant les fichiers suivants :

```
README.md
<hook-name>.json
rpdk.log
src/handler.py
template.yml
```

```
hook-role.yaml
```

En tant que développeur de hooks, vous devez ajouter le type de ressource cible souhaité dans le fichier `<hook-name>.json` de configuration. Dans la configuration ci-dessous, un hook est configuré pour s'exécuter avant qu'une fonction Lambda ne soit créée à l'aide CloudFormation de. Vous pouvez également ajouter des gestionnaires `preUpdate` et des actions `preDelete` similaires.

```
    "handlers": {
        "preCreate": {
            "targetNames": [
                "AWS::Lambda::Function"
            ],
            "permissions": []
        }
    }
```

Vous devez également vous assurer que le CloudFormation hook dispose des autorisations appropriées pour appeler les AWS Config API. Vous pouvez le faire en mettant à jour le fichier de définition de rôle nommé `hook-role.yaml`. Le fichier de définition de rôle possède la politique de confiance suivante par défaut, qui CloudFormation permet d'assumer le rôle.

```
      AssumeRolePolicyDocument:
        Version: '2012-10-17'
        Statement:
          - Effect: Allow
            Principal:
              Service:
                - hooks.cloudformation.amazonaws.com
                - resources.cloudformation.amazonaws.com
```

Pour permettre à ce hook d'appeler des API de configuration, vous devez ajouter les autorisations suivantes à la déclaration de politique. Ensuite, vous soumettez le projet hook à l'aide de la `cfn submit` commande, où vous CloudFormation créez un rôle avec les autorisations requises.

```
      Policies:
        - PolicyName: HookTypePolicy
          PolicyDocument:
            Version: '2012-10-17'
            Statement:
              - Effect: Allow
                Action:
```

```
                  - "config:Describe*"
                  - "config:Get*"
                  - "config:List*"
                  - "config:SelectResourceConfig"
                Resource: "*
```

Ensuite, vous devez écrire une fonction Lambda dans un `src/handler.py` fichier. Dans ce fichier, vous trouverez les méthodes nommées `preCreate`, `preUpdate` et `preDelete` déjà créées lorsque vous avez lancé le projet. Vous souhaitez écrire une fonction commune et réutilisable qui appelle l' AWS Config `StartResourceEvaluation`API en mode proactif à l'aide du AWS SDK pour Python (Boto3). Cet appel d'API prend les propriétés des ressources en entrée et évalue la ressource par rapport à la définition de la règle.

```
def validate_lambda_tracing_config(resource_type, function_properties:
 MutableMapping[str, Any]) -> ProgressEvent:
  LOG.info("Fetching proactive data")
  config_client = boto3.client('config')
  resource_specs = {
      'ResourceId': 'MyFunction',
      'ResourceType': resource_type,
      'ResourceConfiguration': json.dumps(function_properties),
      'ResourceConfigurationSchemaType': 'CFN_RESOURCE_SCHEMA'
  }
  LOG.info("Resource Specifications:", resource_specs)
  eval_response = config_client.start_resource_evaluation(EvaluationMode='PROACTIVE',
 ResourceDetails=resource_specs, EvaluationTimeout=60)
  ResourceEvaluationId = eval_response.ResourceEvaluationId
  compliance_response =
 config_client.get_compliance_details_by_resource(ResourceEvaluationId=ResourceEvaluationId)
  LOG.info("Compliance Verification:",
 compliance_response.EvaluationResults[0].ComplianceType)
  if "NON_COMPLIANT" == compliance_response.EvaluationResults[0].ComplianceType:
      return ProgressEvent(status=OperationStatus.FAILED, message="Lambda function
 found with no tracing enabled : FAILED", errorCode=HandlerErrorCode.NonCompliant)
  else:
      return ProgressEvent(status=OperationStatus.SUCCESS, message="Lambda function
 found with tracing enabled : PASS.")
```

Vous pouvez maintenant appeler la fonction commune depuis le gestionnaire pour le hook de pré-création. Voici un exemple de gestionnaire :

```
@hook.handler(HookInvocationPoint.CREATE_PRE_PROVISION)
```

```
def pre_create_handler(
        session: Optional[SessionProxy],
        request: HookHandlerRequest,
        callback_context: MutableMapping[str, Any],
        type_configuration: TypeConfigurationModel
) -> ProgressEvent:
    LOG.info("Starting execution of the hook")
    target_name = request.hookContext.targetName
    LOG.info("Target Name:", target_name)
    if "AWS::Lambda::Function" == target_name:
        return validate_lambda_tracing_config(target_name,
            request.hookContext.targetModel.get("resourceProperties")
        )
    else:
        raise exceptions.InvalidRequest(f"Unknown target type: {target_name}")
```

Après cette étape, vous pouvez enregistrer le hook et le configurer pour écouter tous les événements de création de AWS Lambda fonctions.

Un développeur prépare le modèle d'infrastructure en tant que code (IaC) pour un microservice sans serveur à l'aide de Lambda. Cette préparation inclut le respect des normes internes, suivi de tests locaux et de validation du modèle dans le référentiel. Voici un exemple de modèle IaC :

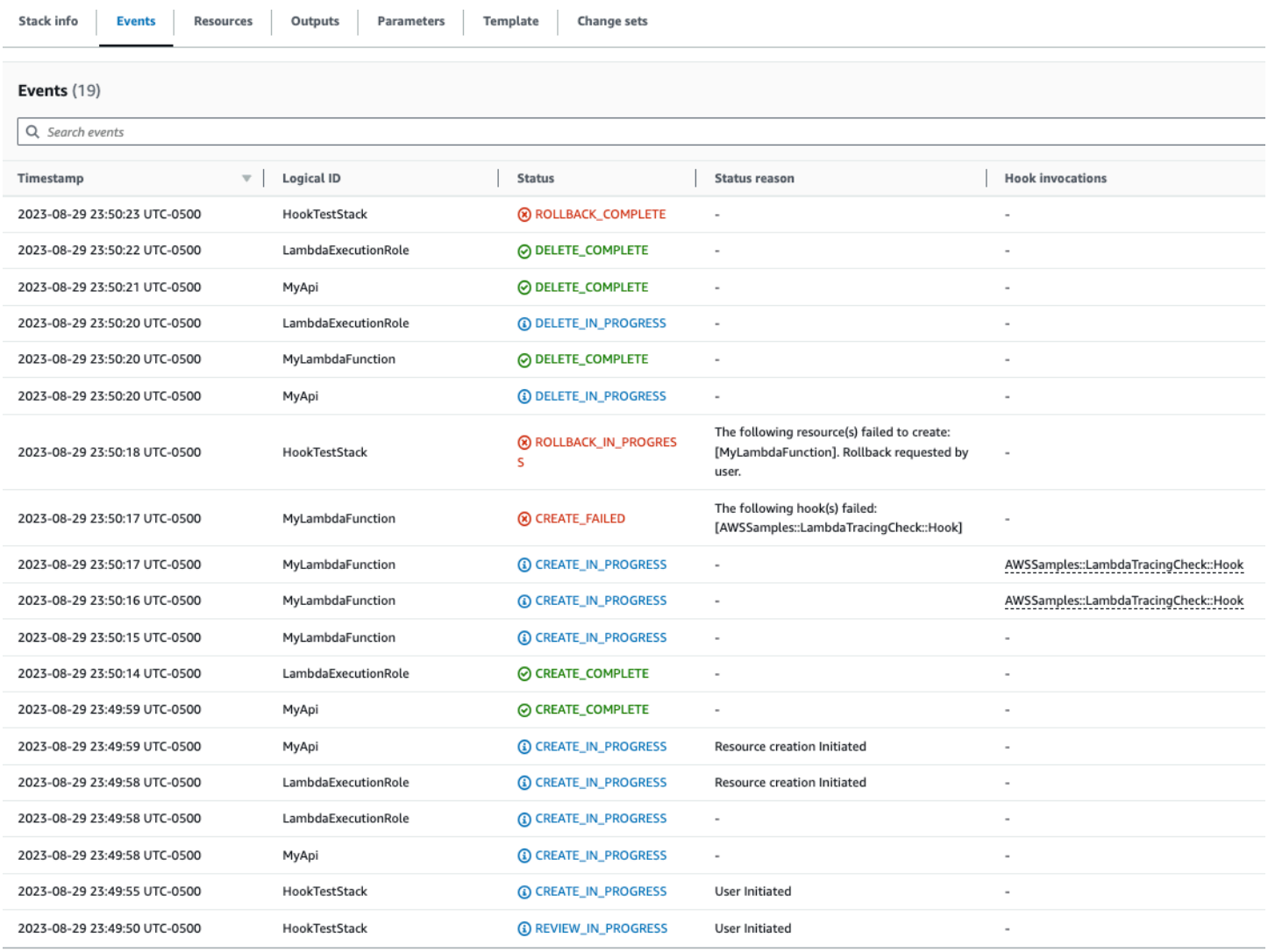
```
  MyLambdaFunction:
  Type: 'AWS::Lambda::Function'
  Properties:
    Handler: index.handler
    Role: !GetAtt LambdaExecutionRole.Arn
    FunctionName: MyLambdaFunction
    Code:
      ZipFile: |
        import json

        def handler(event, context):
            return {
                'statusCode': 200,
                'body': json.dumps('Hello World!')
            }
    Runtime: python3.14
    TracingConfig:
        Mode: PassThrough
    MemorySize: 256
```

```
    Timeout: 10
```

Dans le cadre du CI/CD processus, lorsque le CloudFormation modèle est déployé, le CloudFormation service invoque le create/update pré-hook juste avant de provisionner le type de `AWS::Lambda::Function` ressource. Le hook utilise des AWS Config règles exécutées en mode proactif pour vérifier que la configuration de la fonction Lambda inclut la configuration de suivi obligatoire. La réponse du hook détermine l'étape suivante.

S'il est conforme, le hook signale le succès et CloudFormation procède au provisionnement des ressources. Dans le cas contraire, le déploiement de la CloudFormation pile échoue, le pipeline s'arrête immédiatement et le système enregistre les détails pour un examen ultérieur. Les notifications de conformité sont envoyées vers les parties prenantes concernées.

Vous pouvez trouver les success/fail informations relatives au hook dans la CloudFormation console :



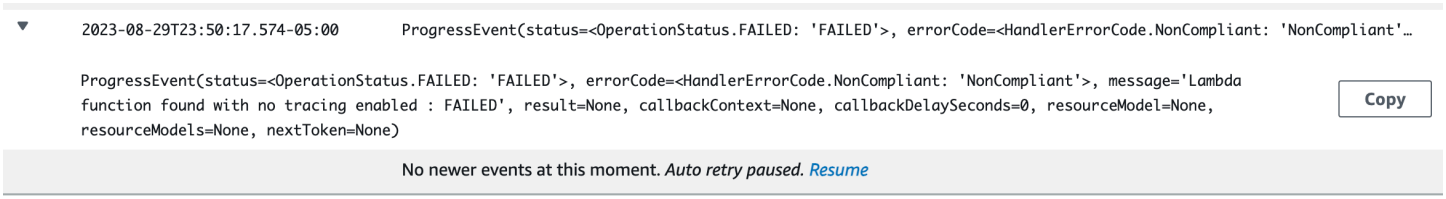
Stack info | Events | Resources | Outputs | Parameters | Template | Change sets

Events (19)

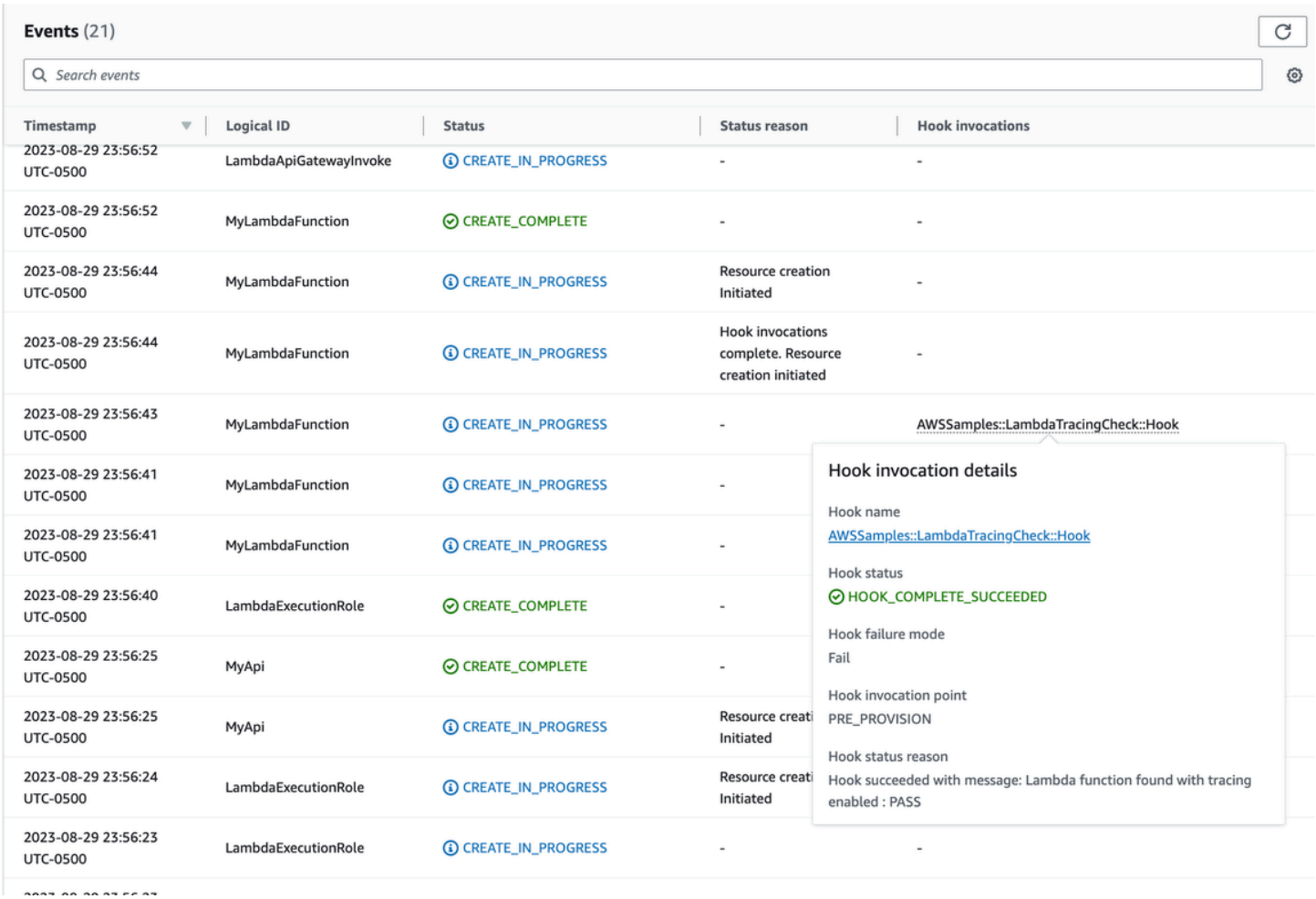
Search events

Timestamp	Logical ID	Status	Status reason	Hook invocations
2023-08-29 23:50:23 UTC-0500	HookTestStack	ROLLBACK_COMPLETE	-	-
2023-08-29 23:50:22 UTC-0500	LambdaExecutionRole	DELETE_COMPLETE	-	-
2023-08-29 23:50:21 UTC-0500	MyApi	DELETE_COMPLETE	-	-
2023-08-29 23:50:20 UTC-0500	LambdaExecutionRole	DELETE_IN_PROGRESS	-	-
2023-08-29 23:50:20 UTC-0500	MyLambdaFunction	DELETE_COMPLETE	-	-
2023-08-29 23:50:20 UTC-0500	MyApi	DELETE_IN_PROGRESS	-	-
2023-08-29 23:50:18 UTC-0500	HookTestStack	ROLLBACK_IN_PROGRESS	The following resource(s) failed to create: [MyLambdaFunction]. Rollback requested by user.	-
2023-08-29 23:50:17 UTC-0500	MyLambdaFunction	CREATE_FAILED	The following hook(s) failed: [AWSSamples::LambdaTracingCheck::Hook]	-
2023-08-29 23:50:17 UTC-0500	MyLambdaFunction	CREATE_IN_PROGRESS	-	AWSSamples::LambdaTracingCheck::Hook
2023-08-29 23:50:16 UTC-0500	MyLambdaFunction	CREATE_IN_PROGRESS	-	AWSSamples::LambdaTracingCheck::Hook
2023-08-29 23:50:15 UTC-0500	MyLambdaFunction	CREATE_IN_PROGRESS	-	-
2023-08-29 23:50:14 UTC-0500	LambdaExecutionRole	CREATE_COMPLETE	-	-
2023-08-29 23:49:59 UTC-0500	MyApi	CREATE_COMPLETE	-	-
2023-08-29 23:49:59 UTC-0500	MyApi	CREATE_IN_PROGRESS	Resource creation Initiated	-
2023-08-29 23:49:58 UTC-0500	LambdaExecutionRole	CREATE_IN_PROGRESS	Resource creation Initiated	-
2023-08-29 23:49:58 UTC-0500	LambdaExecutionRole	CREATE_IN_PROGRESS	-	-
2023-08-29 23:49:58 UTC-0500	MyApi	CREATE_IN_PROGRESS	-	-
2023-08-29 23:49:55 UTC-0500	HookTestStack	CREATE_IN_PROGRESS	User Initiated	-
2023-08-29 23:49:50 UTC-0500	HookTestStack	REVIEW_IN_PROGRESS	User Initiated	-

Si les journaux sont activés pour votre CloudFormation hook, vous pouvez capturer le résultat de l'évaluation du hook. Voici un exemple de journal pour un hook dont l'état a échoué, indiquant que la fonction Lambda n'est pas X-Ray activée :



Si le développeur choisit de modifier le modèle IaC pour mettre à jour la valeur `TracingConfig Mode`sur `Active` et le redéployer, le hook s'exécute correctement et la pile poursuit la création de la ressource Lambda.



De cette façon, vous pouvez mettre en œuvre des contrôles préventifs AWS Config en mode proactif lorsque vous développez et déployez des ressources sans serveur dans vos AWS comptes. En intégrant des AWS Config règles dans le CI/CD pipeline, vous pouvez identifier et éventuellement

bloquer les déploiements de ressources non conformes, tels que les fonctions Lambda qui ne disposent pas d'une configuration de suivi active. Cela garantit que seules les ressources conformes aux dernières politiques de gouvernance sont déployées dans vos AWS environnements.

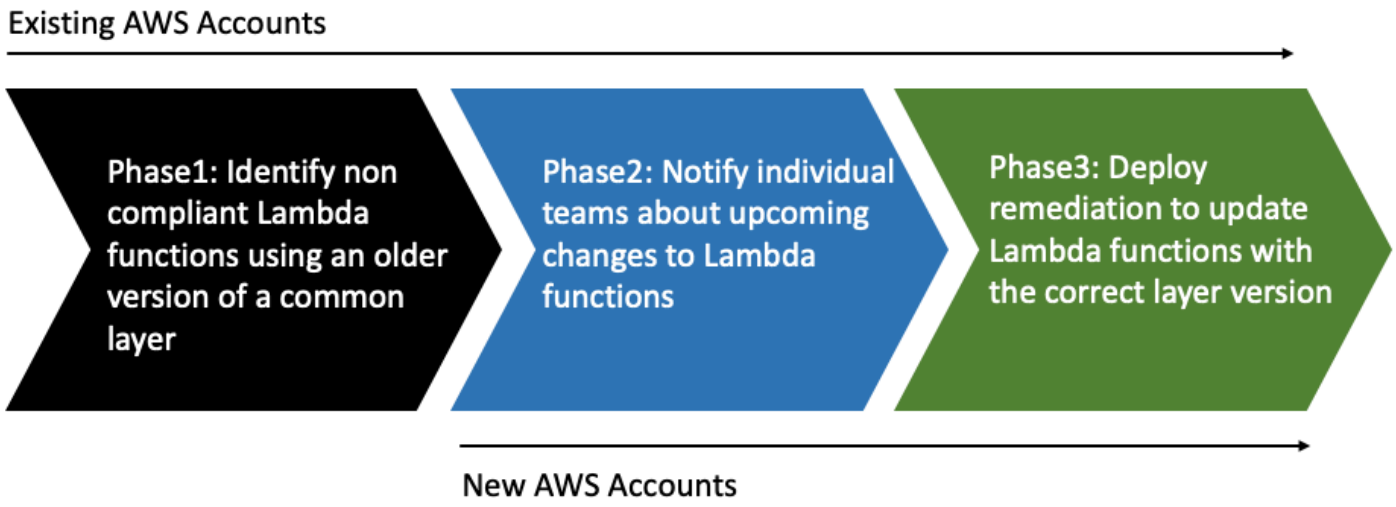
Détectez les déploiements et les configurations Lambda non conformes avec AWS Config

Outre l'évaluation proactive, il AWS Config peut également détecter de manière réactive les déploiements de ressources et les configurations qui ne sont pas conformes à vos politiques de gouvernance. Cela est important car les politiques de gouvernance évoluent au fur et à mesure que votre organisation apprend et met en œuvre de nouvelles meilleures pratiques.

Imaginons un scénario dans lequel vous définissez une toute nouvelle politique lors du déploiement ou de la mise à jour des fonctions Lambda : toutes les fonctions Lambda doivent toujours utiliser une version de couche Lambda spécifique et approuvée. Vous pouvez configurer AWS Config pour surveiller les fonctions nouvelles ou mises à jour pour les configurations de couches. S'il AWS Config détecte une fonction qui n'utilise pas de version de couche approuvée, il signale la fonction comme une ressource non conforme.

Vous pouvez éventuellement configurer AWS Config pour corriger automatiquement la ressource en spécifiant une action de correction à l'aide d'un document d' AWS Systems Manager automatisation. Par exemple, vous pouvez écrire un document d'automatisation en Python à l'aide de AWS SDK pour Python (Boto3), qui met à jour la fonction non conforme pour qu'elle pointe vers la version de couche approuvée. Il AWS Config sert donc à la fois de contrôle de détection et de contrôle correctif, automatisant la gestion de la conformité.

Décomposons ce processus en trois phases de mise en œuvre importantes :



Phase 1 : identification des ressources d'accès

Commencez par l'activer AWS Config sur l'ensemble de vos comptes et configurez-le pour enregistrer les fonctions AWS Lambda. Cela permet d' AWS Config observer quand les fonctions Lambda sont créées ou mises à jour. Vous pouvez ensuite configurer des règles de stratégie personnalisées pour vérifier les violations de politique spécifiques, en utilisant la syntaxe AWS CloudFormation Guard . Les règles de garde prennent la forme générale suivante :

```
rule name when condition { assertion }
```

Vous trouverez ci-dessous un exemple de règle qui vérifie qu'une couche n'est pas définie sur une ancienne version de couche :

```
rule desiredlayer when configuration.layers !empty {
    some configuration.layers[*].arn != CONFIG_RULE_PARAMETERS.OldLayerArn
}
```

Découvrons la syntaxe et la structure des règles :

- Nom de la règle : le nom de la règle est `desiredlayer` dans l'exemple fourni.
- Condition : cette clause spécifie la condition dans laquelle la règle doit être vérifiée. Dans l'exemple fourni, la condition est `configuration.layers !empty`. Cela signifie que la ressource ne doit être évaluée que lorsque la propriété `layers` de la configuration n'est pas vide.
- Assertion : après la clause `when`, une assertion détermine ce que la règle vérifie. L'assertion `some configuration.layers[*].arn != CONFIG_RULE_PARAMETERS.OldLayerArn` vérifie si l'un des ARN de la couche Lambda ne correspond pas à la valeur `OldLayerArn`. S'ils ne correspondent pas, l'assertion est vraie et la règle est acceptée ; sinon, elle échoue.

`CONFIG_RULE_PARAMETERS`est un ensemble spécial de paramètres configuré avec la AWS Config règle. Dans ce cas, `OldLayerArn` est un paramètre dans `CONFIG_RULE_PARAMETERS`. Cela permet aux utilisateurs de fournir une valeur d'ARN spécifique qu'ils considèrent comme ancienne ou obsolète, puis la règle vérifie si des fonctions Lambda utilisent cet ancien ARN.

Phase 2 : Visualisation et conception

AWS Config rassemble les données de configuration et les stocke dans des compartiments Amazon Simple Storage Service (Amazon S3). Vous pouvez utiliser Amazon Athena pour interroger ces

données directement depuis vos compartiments S3. Avec Athena, vous pouvez agréger ces données au niveau de l'organisation, en générant une vue globale de la configuration de vos ressources sur l'ensemble de vos comptes. Pour configurer l'agrégation des données de configuration des ressources, consultez Visualisation AWS Config des données à l'aide d'Athena et d'Amazon Quick sur le blog AWS Cloud Operations and Management.

Voici un exemple de requête Athena pour identifier toutes les fonctions Lambda à l'aide d'un ARN de couche particulier :

```
WITH unnested AS (
    SELECT
      item.awsaccountid AS account_id,
      item.awsregion AS region,
      item.configuration AS lambda_configuration,
      item.resourceid AS resourceid,
      item.resourcename AS resourcename,
      item.configuration AS configuration,
      json_parse(item.configuration) AS lambda_json
    FROM
      default.aws_config_configuration_snapshot,
      UNNEST(configurationitems) as t(item)
    WHERE
      "dt" = 'latest'
      AND item.resourcetype = 'AWS::Lambda::Function'
  )

  SELECT DISTINCT
    region as Region,
    resourcename as FunctionName,
    json_extract_scalar(lambda_json, '$.memorySize') AS memory_size,
    json_extract_scalar(lambda_json, '$.timeout') AS timeout,
    json_extract_scalar(lambda_json, '$.version') AS version
  FROM
    unnested
  WHERE
    lambda_configuration LIKE '%arn:aws:lambda:us-
east-1:111122223333:layer:AnyGovernanceLayer:24%'
```

Voici les résultats de la requête :

Query results | Query stats

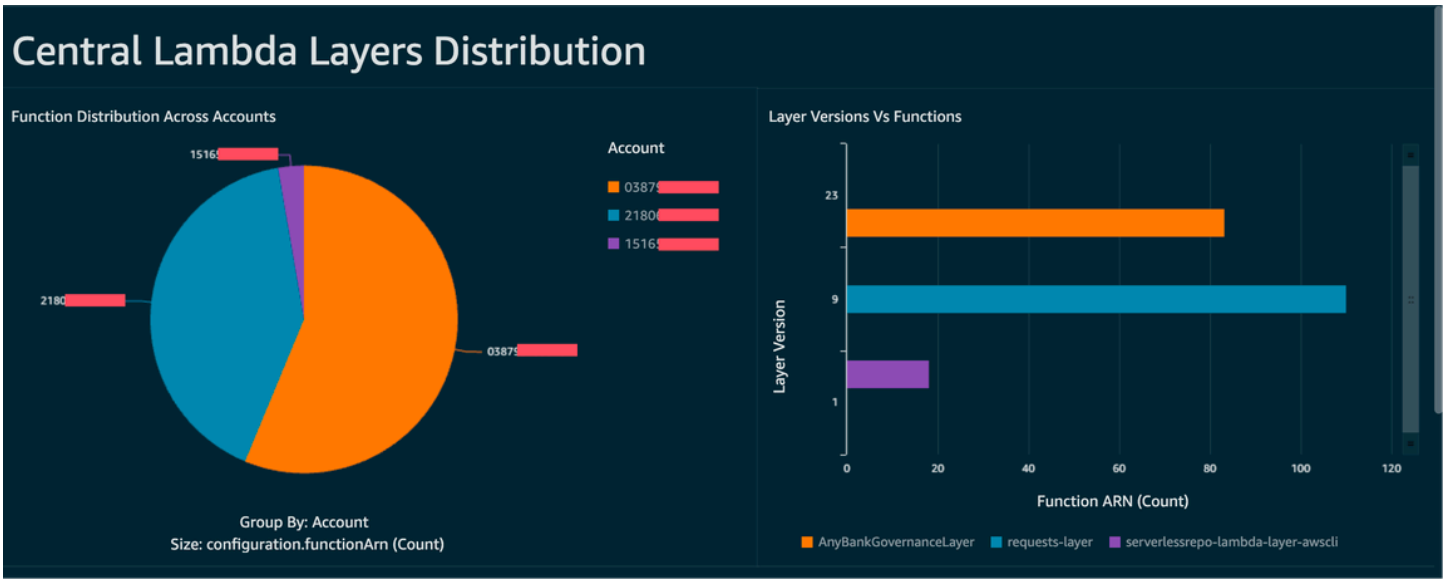
Completed — Time in queue: 127 ms — Run time: 1.803 sec — Data scanned: 239.40 KB

Results (27) — Copy — Download results

Search rows — 1

#	Region	FunctionName	memory_size	timeout	version
1	us-east-1	UpdateUIForPublishEvents	128	18	$LATEST
2	us-east-1	SchedulerCLI-InstanceSchedulerMain	128	300	$LATEST
3	us-east-1	my_functions_function10	128	3	$LATEST
4	us-east-1	lex-web-ui-CognitoIdentityP-CleanStackNameFunction-1TSORSH6L6YXQ	128	300	$LATEST
5	us-east-1	GetLatestArn	128	3	$LATEST
6	us-east-1	aws-python-http-api-project-dev-hello	1024	6	$LATEST
7	us-east-1	cloud9-MyTest-MyTest-688JGPVYP37L	128	15	$LATEST
8	us-east-1	my_functions_function1	128	3	$LATEST
9	us-east-1	my_functions_function25	128	3	$LATEST

Une fois les AWS Config données agrégées au sein de l'organisation, vous pouvez ensuite créer un tableau de bord à l'aide d'Amazon Quick. En important vos résultats Athena dans Quick, vous pouvez visualiser dans quelle mesure vos fonctions Lambda respectent la règle de version des couches. Ce tableau de bord peut mettre en évidence les ressources conformes et non conformes, ce qui vous aide à déterminer votre politique d'application, comme indiqué dans la section suivante. L'image suivante est un exemple de tableau de bord qui indique la distribution des versions de couches appliquées aux fonctions au sein de l'organisation.



Phase 3 : mettre en œuvre et appliquer

Vous pouvez désormais associer votre règle de version de couche que vous avez créée au cours de la phase 1 à une action de correction via un document d'automatisation de Systems Manager, que vous créez sous la forme d'un script Python écrit avec AWS SDK pour Python (Boto3). Le script

appelle l'action d'UpdateFunctionConfigurationAPI pour chaque fonction Lambda, en mettant à jour la configuration de la fonction avec la nouvelle couche ARN. Vous pouvez également demander au script de soumettre une pull request au référentiel de code pour mettre à jour l'ARN de la couche. De cette façon, les futurs déploiements de code sont également mis à jour avec le bon ARN de couche.

Signature de code Lambda avec AWS Signer

AWS Signerest un service de signature de code entièrement géré que vous pouvez utiliser pour valider votre code par rapport à une signature numérique afin de confirmer que le code n'a pas été modifié et qu'il provient d'un éditeur de confiance. AWS Signer peut être utilisé conjointement AWS Lambda pour vérifier que les fonctions et les couches ne sont pas modifiées avant le déploiement dans vos AWS environnements. Cela protège votre organisation contre les acteurs malveillants susceptibles d'avoir obtenu des informations d'identification pour créer de nouvelles fonctions ou mettre à jour des fonctions existantes.

Pour configurer la signature de code pour vos fonctions Lambda, commencez par créer un compartiment S3 avec la gestion des versions activée. Ensuite, créez un profil de signature avec AWS Signer, spécifiez Lambda comme plate-forme, puis spécifiez une période de jours pendant laquelle le profil de signature est valide. Exemple :

```
Signer:
  Type: AWS::Signer::SigningProfile
  Properties:
    PlatformId: AWSLambda-SHA384-ECDSA
    SignatureValidityPeriod:
      Type: DAYS
      Value: !Ref pValidDays
```

Utilisez ensuite le profil de signature et créez une configuration de signature avec Lambda. Vous devez spécifier ce qu'il convient de faire lorsque la configuration de signature détecte un artefact qui ne correspond pas à la signature numérique attendue : avertir (mais autoriser le déploiement) ou appliquer (et bloquer le déploiement). L'exemple ci-dessous est configuré pour appliquer et bloquer les déploiements.

```
SigningConfig:
  Type: AWS::Lambda::CodeSigningConfig
  Properties:
    AllowedPublishers:
      SigningProfileVersionArns:
        - !GetAtt Signer.ProfileVersionArn
    CodeSigningPolicies:
      UntrustedArtifactOnDeployment: Enforce
```

Vous avez maintenant AWS Signer configuré Lambda pour bloquer les déploiements non fiables. Supposons que vous avez terminé de coder une demande de fonctionnalité et que vous êtes

maintenant prêt à déployer la fonction. La première étape consiste à compresser le code avec les dépendances appropriées, puis à signer l'artefact à l'aide du profil de signature que vous avez créé. Vous pouvez le faire en téléchargeant l'artefact zip dans le compartiment S3, puis en lançant une tâche de signature.

```
aws signer start-signing-job \
--source 's3={bucketName=your-versioned-bucket,key=your-prefix/your-zip-
artifact.zip,version=QyaJ3c4qa50LXV.9VaZgXHlsGbvCXxpT}' \
--destination 's3={bucketName=your-versioned-bucket,prefix=your-prefix/}' \
--profile-name your-signer-id
```

Vous obtenez une sortie comme suit, où `jobId` est l'objet créé dans le compartiment et le préfixe de destination et l' Compte AWS identifiant à 12 chiffres sur lequel la tâche a été exécutée. `jobOwner`

```
{
    "jobId": "87a3522b-5c0b-4d7d-b4e0-4255a8e05388",
    "jobOwner": "111122223333"
  }
```

Vous pouvez désormais déployer votre fonction à l'aide de l'objet S3 signé et de la configuration de signature de code que vous avez créée.

```
  Fn:
    Type: AWS::Serverless::Function
    Properties:
      CodeUri: s3://your-versioned-bucket/your-prefix/87a3522b-5c0b-4d7d-
b4e0-4255a8e05388.zip
      Handler: fn.handler
      Role: !GetAtt FnRole.Arn
      CodeSigningConfigArn: !Ref pSigningConfigArn
```

Vous pouvez également tester le déploiement d'une fonction avec l'artefact zip source non signé d'origine. Le déploiement devrait échouer avec le message d'erreur suivant : .

```
Lambda cannot deploy the function. The function or layer might be signed using a
 signature that the client is not configured to accept. Check the provided signature
 for unsigned.
```

Si vous créez et déployez vos fonctions à l'aide du AWS Serverless Application Model (AWS SAM), la commande du package gère le téléchargement de l'artefact zip vers S3 et démarre également la

tâche de signature et obtient l'artefact signé. Pour ce faire, vous pouvez utiliser la commande avec les paramètres suivants :

```
sam package -t your-template.yaml \
--output-template-file your-output.yaml \
--s3-bucket your-versioned-bucket \
--s3-prefix your-prefix \
--signing-profiles your-signer-id
```

AWS Signer vous permet de vérifier que les artefacts zip déployés sur vos comptes sont fiables pour le déploiement. Vous pouvez inclure le processus ci-dessus dans vos CI/CD pipelines et exiger que toutes les fonctions soient associées à une configuration de signature de code en utilisant les techniques décrites dans les rubriques précédentes. En utilisant la signature de code dans vos déploiements de fonctions Lambda, vous empêchez les acteurs malveillants susceptibles d'avoir obtenu des informations d'identification pour créer ou mettre à jour des fonctions d'injecter du code malveillant dans vos fonctions.

Automatisation des évaluations de sécurité pour Lambda avec Amazon Inspector

Amazon Inspector est un service de gestion des vulnérabilités qui analyse continuellement les charges de travail pour détecter les vulnérabilités logicielles connues et l'exposition involontaire au réseau. Amazon Inspector crée une constatation qui décrit la vulnérabilité, identifie la ressource affectée, évalue la gravité de la vulnérabilité et fournit des conseils pour y remédier.

Le support d'Amazon Inspector fournit une évaluation automatique et continue des vulnérabilités de sécurité pour les fonctions et les couches Lambda. Amazon Inspector propose deux types de scan pour Lambda :

- Analyse standard Lambda (par défaut) : analyse les dépendances des applications au sein d'une fonction Lambda et de ses couches pour détecter les vulnérabilités des packages.
- Analyse du code Lambda : analyse le code d'application personnalisé dans vos fonctions et couches pour détecter les vulnérabilités du code. Vous pouvez activer l’analyse standard Lambda ou activer l’analyse standard Lambda conjointement avec l’analyse du code Lambda.

Pour activer Amazon Inspector, accédez à la console Amazon Inspector, développez la section Paramètres et choisissez Gestion des comptes. Dans l'onglet Comptes, choisissez Activer, puis sélectionnez l'une des options d’analyse.

Vous pouvez activer Amazon Inspector pour plusieurs comptes et déléguer les autorisations de gestion d'Amazon Inspector pour l'organisation à des comptes spécifiques lors de la configuration d'Amazon Inspector. Lors de l'activation, vous devez accorder des autorisations à Amazon Inspector en créant le rôle :`AWSServiceRoleForAmazonInspector2`. Dans la console Amazon Inspector, vous pouvez créer ce rôle à l'aide d'une option en une seule étape.

Pour l'analyse standard Lambda, Amazon Inspector lance des analyses de vulnérabilité des fonctions Lambda dans les situations suivantes :

- Dès qu'Amazon Inspector découvre une fonction Lambda existante.
- Lorsque vous déployez une fonction Lambda.
- Lorsque vous déployez une mise à jour du code d'application ou des dépendances d'une fonction Lambda existante ou de ses couches.
- Chaque fois qu'Amazon Inspector ajoute un nouvel élément Common Vulnerabilities and Exposures (CVE) à sa base de données, et que ce CVE est pertinent pour votre fonction.

Pour l’analyse du code Lambda, Amazon Inspector évalue le code d'application de votre fonction Lambda à l'aide d'un raisonnement automatisé et d'un machine learning qui analyse le code de votre application pour vérifier sa conformité globale en matière de sécurité. Si Amazon Inspector détecte une vulnérabilité dans le code d'application de votre fonction Lambda, Amazon Inspector produit une recherche détaillée de vulnérabilité dans le code. Pour obtenir la liste des détections possibles, consultez la bibliothèque https://docs.aws.amazon.com/codeguru/detector-library/ Amazon CodeGuru Detector.

Pour consulter les résultats, rendez-vous sur la console Amazon Inspector. Dans le menu Résultats, choisissez Par fonction Lambda pour afficher les résultats de l’analyse de sécurité effectuée sur les fonctions Lambda.

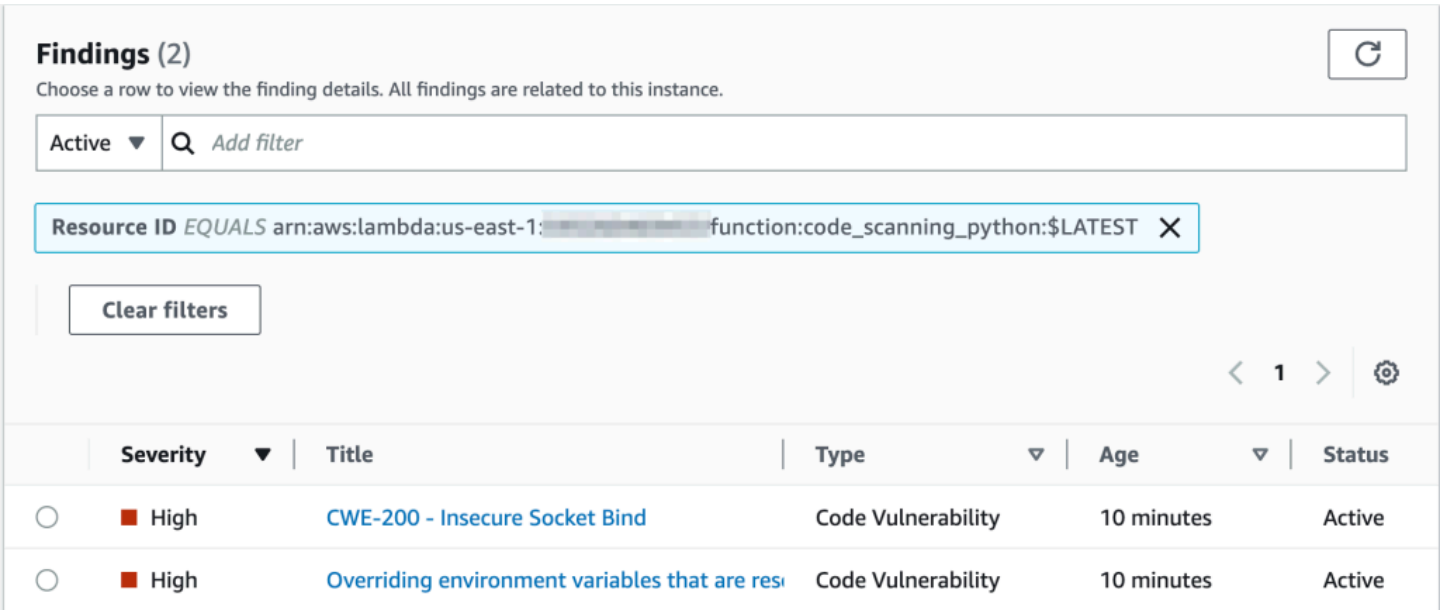
Pour exclure une fonction Lambda de l’analyse standard, balisez la fonction avec la paire clé-valeur suivante :

- `Key:InspectorExclusion`
- `Value:LambdaStandardScanning`

Pour exclure une fonction Lambda des analyses du code, balisez la fonction avec la paire clé-valeur suivante :

- `Key:InspectorCodeExclusion`
- `Value:LambdaCodeScanning`

Par exemple, comme le montre l'image suivante, Amazon Inspector détecte automatiquement les vulnérabilités et classe les résultats de type Vulnérabilité de code, ce qui indique que la vulnérabilité se trouve dans le code de la fonction, et non dans l'une des bibliothèques dépendantes du code. Vous pouvez vérifier ces informations pour une fonction spécifique ou pour plusieurs fonctions à la fois.



Vous pouvez approfondir chacun de ces résultats et découvrir comment remédier au problème.

Overriding environment variables that are reserved by AWS Lambda might lead to unexpected behavior.

Finding ID: arn:aws:inspector2:us-east-1:[redacted]:finding/[redacted]

Overriding environment variables that are reserved by AWS Lambda might lead to unexpected behavior or failure of the Lambda function.

Finding overview	
AWS account ID	[redacted]
Severity	High
Type	Code Vulnerability
Detector name	Override of reserved variable names in a Lambda function
Relevant CWE	--
Rule ID	Rule-434311
Detector tags	#availability, #aws-python-sdk, #aws-lambda, #data-integrity, #maintainability, #security, #security-context, #python
Fix available	Yes
Created at	March 29, 2023 10:08 AM (UTC-04:00)

Vulnerability details	
File path	lambda_function.py

Vulnerability location

```
3  import socket
4
5  def lambda_handler(event, context):
6
7      # print("Scenario 1");
8      os.environ['_HANDLER'] = 'hello'
9      # print("Scenario 1 ends")
10
11     # print("Scenario 2");
12     s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
13     s.bind(('',0))
```

Suggested remediation

Your code attempts to override an environment variable that is reserved by the Lambda runtime environment. This can lead to unexpected behavior and might break the execution of your Lambda function.

Lorsque vous travaillez avec vos fonctions Lambda, assurez-vous de respecter les conventions de dénomination de vos fonctions Lambda. Pour de plus amples informations, veuillez consulter Utilisation des variables d'environnement Lambda.

Vous êtes responsable des suggestions de correction que vous acceptez. Passez toujours en revue les suggestions de correction avant de les accepter. Vous devrez peut-être apporter des modifications aux suggestions de correction pour vous assurer que votre code répond à vos attentes.

Mettre en œuvre l'observabilité pour la sécurité et la conformité Lambda

AWS Config est un outil utile pour trouver et corriger les ressources AWS Serverless non conformes. Chaque modification que vous apportez à vos ressources sans serveur est enregistrée dans AWS Config. De plus, avec AWS Config, vous pouvez stocker les données d'instantané de configuration sur S3.

Vous pouvez utiliser Amazon Athena et Amazon Quick pour créer des tableaux de bord et consulter AWS Config des données. Dans Détectez les déploiements et les configurations Lambda non conformes avec AWS Config, nous avons discuté de la manière dont nous pouvons visualiser une certaine configuration, comme les couches Lambda. Cette rubrique développe ces concepts.

Visibilité sur les configurations Lambda

Vous pouvez utiliser des requêtes pour extraire des configurations importantes telles que l' Compte AWS ID, la région, la configuration de AWS X-Ray suivi, la configuration du VPC, la taille de la mémoire, le temps d'exécution et les balises. Voici un exemple de requête que vous pouvez utiliser pour extraire ces informations d'Athena :

```
WITH unnested AS (
    SELECT
      item.awsaccountid AS account_id,
      item.awsregion AS region,
      item.configuration AS lambda_configuration,
      item.resourceid AS resourceid,
      item.resourcename AS resourcename,
      item.configuration AS configuration,
      json_parse(item.configuration) AS lambda_json
    FROM
      default.aws_config_configuration_snapshot,
      UNNEST(configurationitems) as t(item)
    WHERE
      "dt" = 'latest'
      AND item.resourcetype = 'AWS::Lambda::Function'
  )

  SELECT DISTINCT
    account_id,
    tags,
    region as Region,
    resourcename as FunctionName,
```

```
    json_extract_scalar(lambda_json, '$.memorySize') AS memory_size,
    json_extract_scalar(lambda_json, '$.timeout') AS timeout,
    json_extract_scalar(lambda_json, '$.runtime') AS version
    json_extract_scalar(lambda_json, '$.vpcConfig.SubnetIds') AS vpcConfig
    json_extract_scalar(lambda_json, '$.tracingConfig.mode') AS tracingConfig
  FROM
    unnested
```

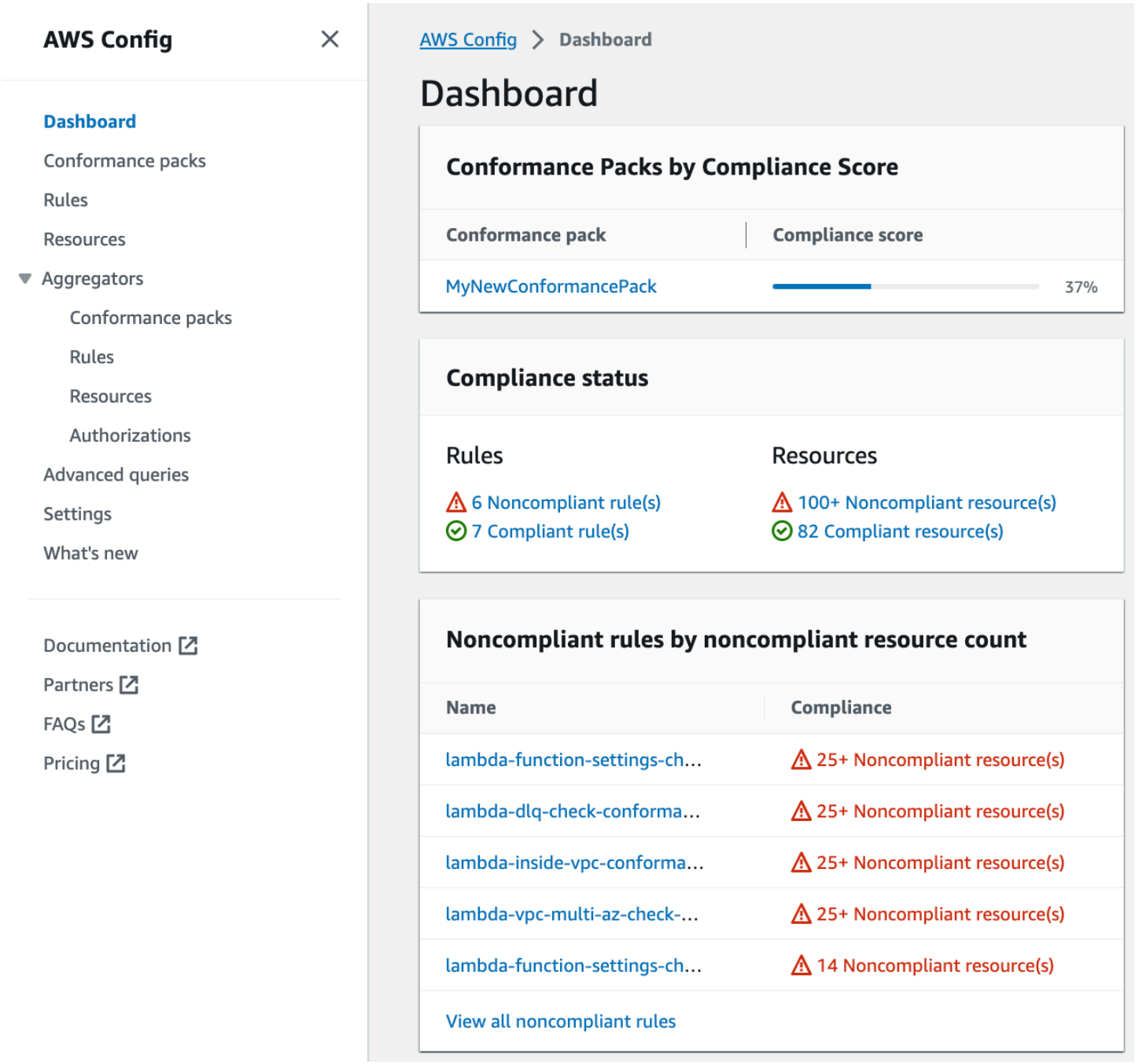
Vous pouvez utiliser la requête pour créer un tableau de bord rapide et visualiser les données. Pour agréger les données de configuration des AWS ressources, créer des tableaux dans Athena et créer des tableaux de bord rapides à partir des données d'Athena, consultez Visualisation des AWS Config données à l'aide d'Athena et d'Amazon Quick sur le blog AWS Cloud Operations and Management. Notamment, cette requête récupère également les informations de balise pour les fonctions. Cela permet de mieux comprendre vos charges de travail et vos environnements, en particulier si vous utilisez des balises personnalisées.

Pour plus d'informations sur les actions que vous pouvez entreprendre, consultez la section Prise en compte des constatations relatives à l'observabilité plus loin dans cette rubrique.

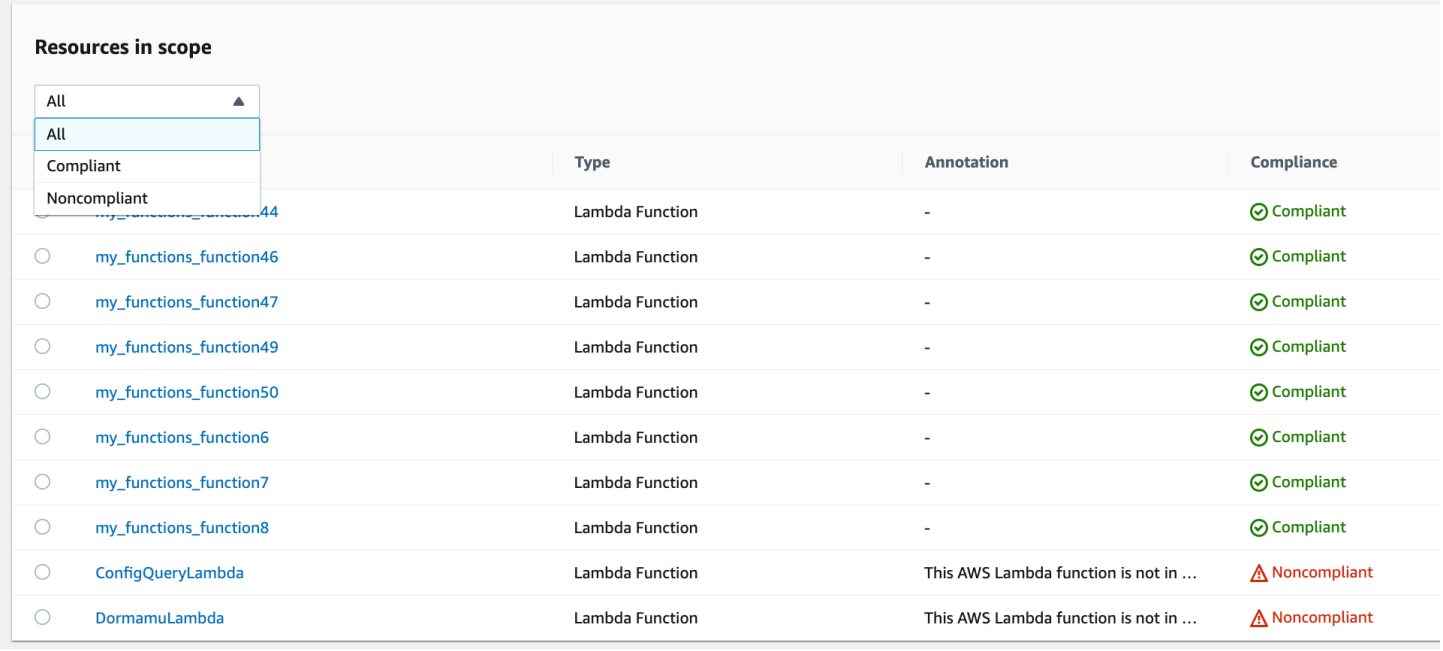
Visibilité sur la conformité à Lambda

À l'aide des données générées par AWS Config, vous pouvez créer des tableaux de bord au niveau de l'organisation pour contrôler la conformité. Cela permet un suivi et une surveillance cohérents de :

- Packs de conformité par score de conformité
- Règles en fonction des ressources non conformes
- Statut de conformité

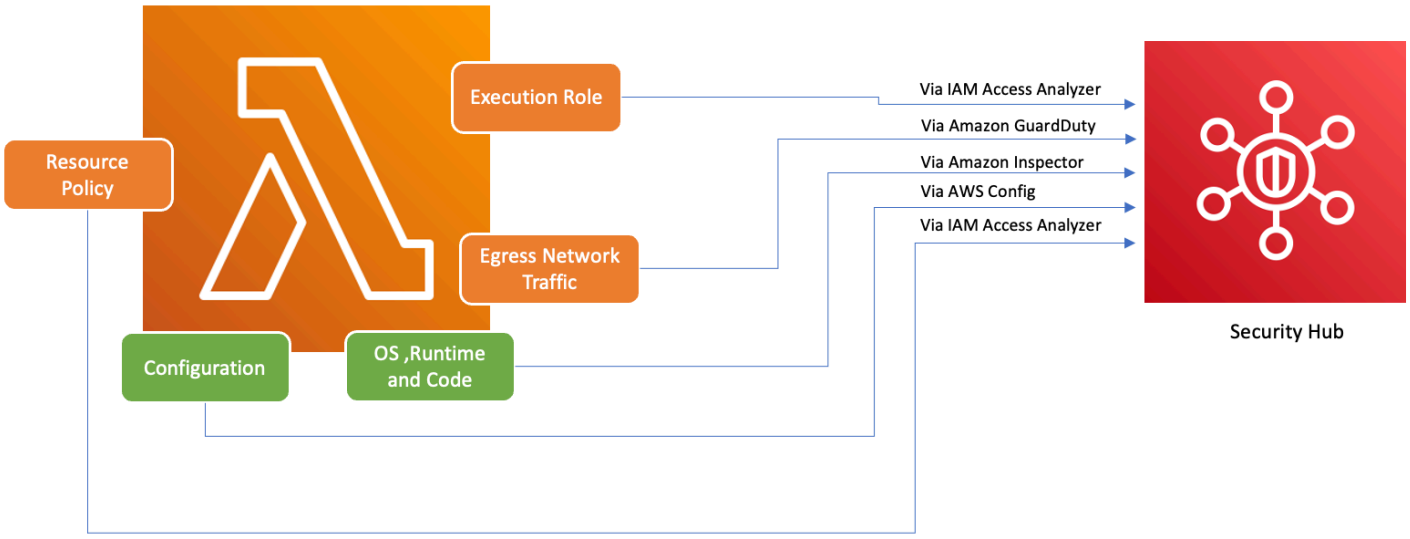


Vérifiez chaque règle pour identifier les ressources non conformes à cette règle. Par exemple, si votre organisation exige que toutes les fonctions Lambda soient associées à un VPC et si vous avez déployé une AWS Config règle pour identifier la conformité, vous pouvez sélectionner la `lambda-inside-vpc` règle dans la liste ci-dessus.



Pour plus d'informations sur les actions que vous pouvez entreprendre, consultez la section [Prise en compte des constatations relatives à l'observabilité] ci-dessous.

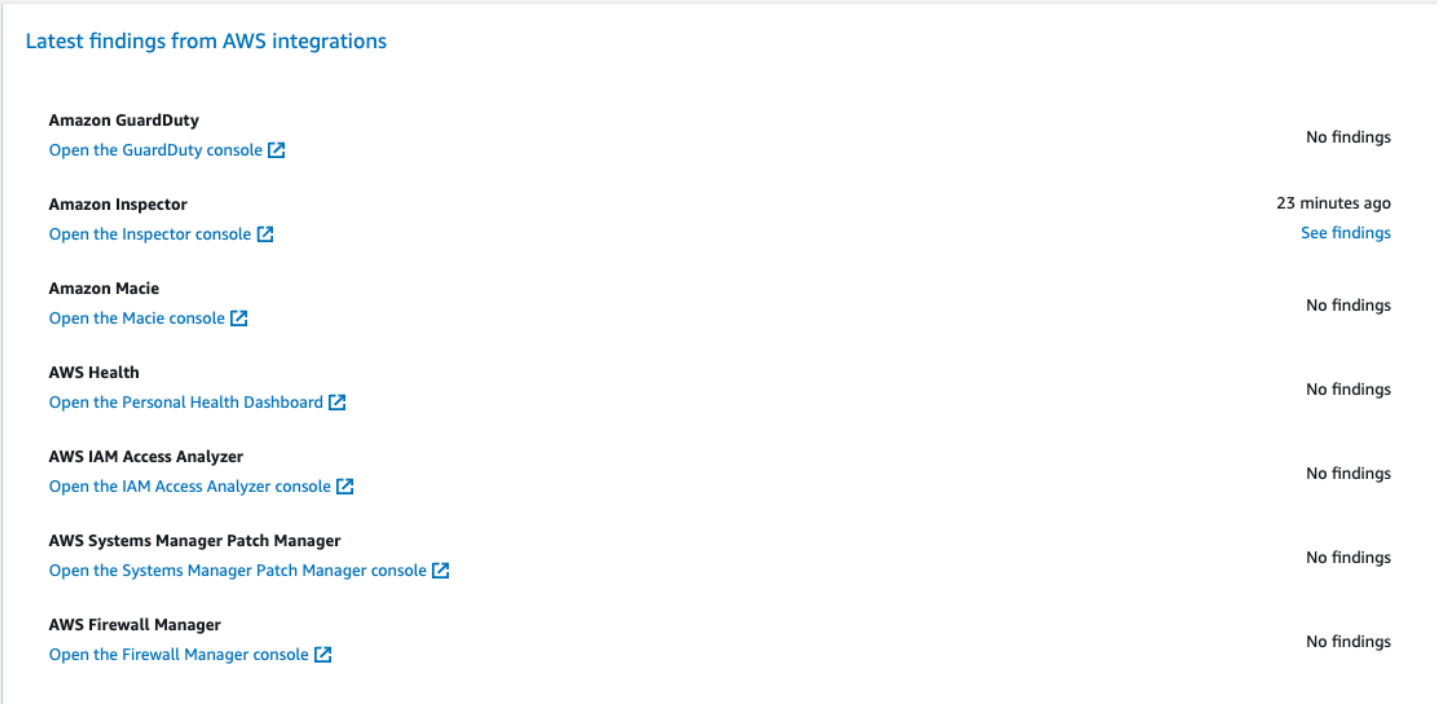
Visibilité des limites des fonctions Lambda à l'aide de Security Hub CSPM



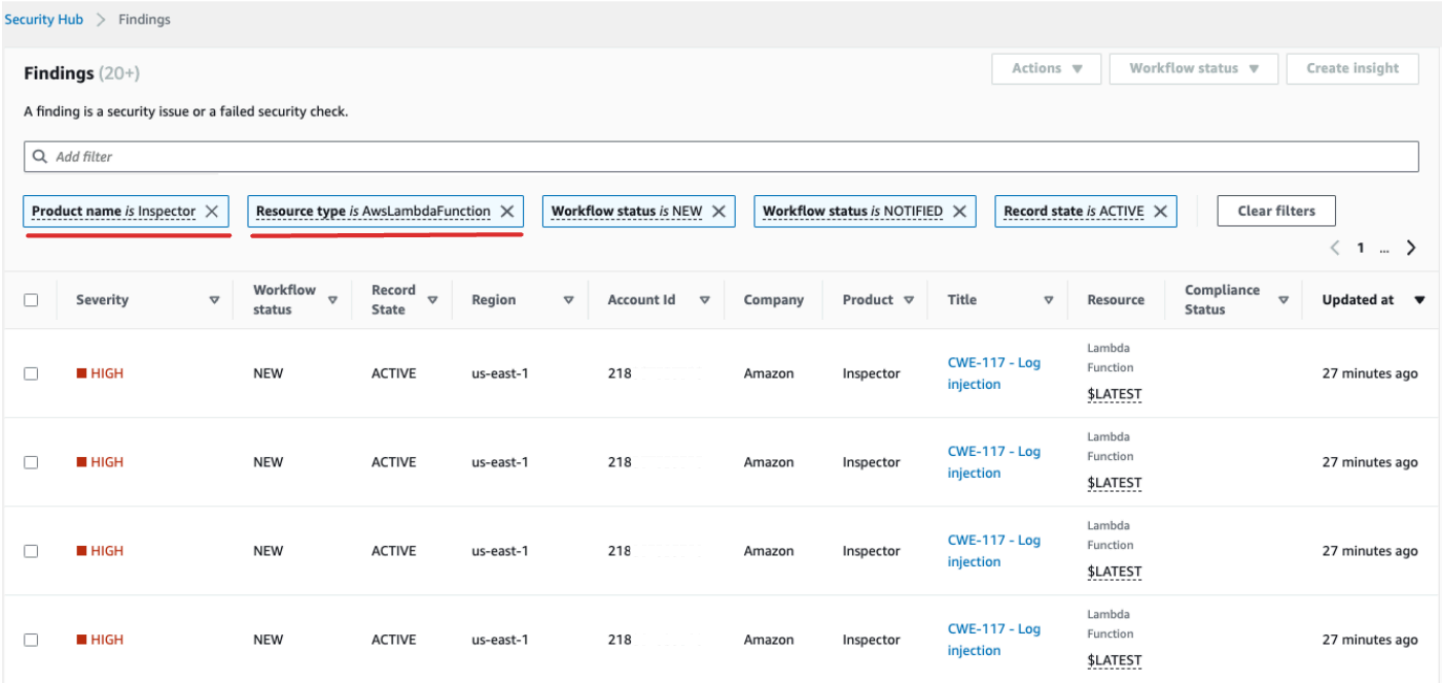
Pour garantir que les AWS services tels que Lambda sont utilisés en toute sécurité, AWS a introduit les meilleures pratiques de sécurité fondamentales v1.0.0. Cet ensemble de bonnes pratiques fournit des directives claires pour la sécurisation des ressources et des données dans l' AWS environnement, en soulignant l'importance de maintenir une posture de sécurité solide. Il AWS Security Hub CSPM complète cela en proposant un centre de sécurité et de conformité unifié. Il

regroupe, organise et hiérarchise les résultats de sécurité provenant de plusieurs AWS services tels qu'Amazon Inspector et AWS Identity and Access Management Access Analyzer Amazon. GuardDuty

Si Security Hub CSPM, Amazon Inspector, IAM Access Analyzer sont GuardDuty activés au sein de votre AWS organisation, Security Hub CSPM regroupe automatiquement les résultats de ces services. Prenons par exemple Amazon Inspector. À l'aide de Security Hub CSPM, vous pouvez identifier efficacement les vulnérabilités du code et des packages dans les fonctions Lambda. Dans la console Security Hub CSPM, accédez à la section inférieure intitulée Les derniers résultats des AWS intégrations. Vous pouvez y consulter et analyser les résultats provenant de divers AWS services intégrés.



Pour voir les détails, cliquez sur le lien Voir les résultats dans la deuxième colonne. Cela affiche une liste des résultats filtrés par produit, comme Amazon Inspector. Pour limiter votre recherche aux fonctions Lambda, définissez `ResourceType` sur `AwsLambdaFunction`. Cela affiche les résultats d'Amazon Inspector relatifs aux fonctions Lambda.



Pour GuardDuty, vous pouvez identifier les modèles de trafic réseau suspects. De telles anomalies peuvent suggérer l'existence d'un code potentiellement malveillant dans votre fonction Lambda.

Avec IAM Access Analyzer, vous pouvez vérifier les politiques, en particulier celles comportant des instructions de condition qui accordent l'accès aux fonctions à des entités externes. De plus, IAM Access Analyzer évalue les autorisations définies lors de l'utilisation de l'AddPermissionopération dans l'API Lambda à côté d'un. `EventSourceToken`

Prise en compte des constatations relatives à l'observabilité

Compte tenu du large éventail de configurations possibles pour les fonctions Lambda et de leurs exigences distinctes, une solution d'automatisation standardisée pour la correction peut ne pas convenir à toutes les situations. De plus, les modifications sont mises en œuvre différemment selon les environnements. Si vous rencontrez une configuration qui ne semble pas conforme, tenez compte des directives suivantes :

1. Stratégie de balisage

   Nous vous recommandons de mettre en œuvre une stratégie de balisage complète. Chaque fonction Lambda doit être étiquetée avec des informations clés telles que :

   - Propriétaire : personne ou équipe responsable de la fonction.
   - Environnement : production, mise en scène, développement ou bac à sable.

- Application : le contexte plus large auquel appartient cette fonction, le cas échéant.

2. Sensibilisation des propriétaires

   Au lieu d'automatiser les modifications majeures (comme l'ajustement de la configuration du VPC), contactez de manière proactive les propriétaires des fonctions non conformes (identifiées par le tag du propriétaire) en leur laissant suffisamment de temps pour :

   - Ajuster les configurations non conformes sur les fonctions Lambda.
   - Fournir une explication et demander une exception, ou affiner les normes de conformité.

3. Gestion d'une base de gestion des configurations (CMDB)

   Bien que les balises puissent fournir un contexte immédiat, le maintien d'une CMDB centralisée peut fournir des informations plus approfondies. Il peut contenir des informations plus détaillées sur chaque fonction Lambda, ses dépendances et d'autres métadonnées critiques. Une CMDB est une ressource inestimable pour les audits, les contrôles de conformité et l'identification des responsables des fonctions.

Le paysage de l'infrastructure sans serveur étant en constante évolution, il est essentiel d'adopter une position proactive en matière de surveillance. Grâce à des outils tels que AWS Config Security Hub CSPM et Amazon Inspector, les anomalies potentielles ou les configurations non conformes peuvent être rapidement identifiées. Cependant, les outils ne peuvent à eux seuls garantir une conformité totale ou des configurations optimales. Il est essentiel d'associer ces outils à des processus bien documentés et aux meilleures pratiques.

- Boucle de rétroaction : une fois les étapes de correction entreprises, assurez-vous qu'il existe une boucle de rétroaction. Cela implique de revoir régulièrement les ressources non conformes pour vérifier si elles ont été mises à jour ou si elles présentent toujours les mêmes problèmes.
- Documentation : documentez toujours les observations, les mesures prises et les exceptions accordées. Une documentation appropriée aide non seulement lors des audits, mais contribue également à améliorer le processus afin d'améliorer la conformité et la sécurité à l'avenir.
- Formation et sensibilisation : assurez-vous que toutes les parties prenantes, en particulier les responsables des fonctions Lambda, sont régulièrement formées et informées des meilleures pratiques, des politiques organisationnelles et des mandats de conformité. Des ateliers, des webinaires ou des sessions de formation réguliers peuvent contribuer dans une large mesure à garantir que tout le monde est sur la même longueur d'onde en matière de sécurité et de conformité.

En conclusion, alors que les outils et les technologies fournissent des capacités robustes pour détecter et signaler les problèmes potentiels, l'élément humain (compréhension, communication, formation et documentation) reste essentiel. Ensemble, ils forment une puissante combinaison qui garantit que vos fonctions Lambda et votre infrastructure globale restent conformes, sécurisées et optimisées pour répondre aux besoins de votre entreprise.

Validation de conformité pour AWS Lambda

Third-party les auditeurs évaluent la sécurité et la conformité dans AWS Lambda le cadre de multiples programmes de AWS conformité. Il s'agit notamment des certifications SOC, PCI, FedRAMP, HIPAA et d'autres.

Pour une liste des AWS services couverts par des programmes de conformité spécifiques, voir les AWS services concernés par programme de conformité. Pour obtenir des informations générales, veuillez consulter Programmes de conformité d'AWS.

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, consultez Téléchargement de rapports dans AWS Artifact.

Votre responsabilité de conformité lors de l'utilisation de Lambda est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise, ainsi que par la législation et la réglementation applicables. Vous pouvez mettre en œuvre des contrôles de gouvernance pour garantir que les fonctions Lambda de votre entreprise répondent à vos exigences de conformité. Pour de plus amples informations, veuillez consulter Création d'une stratégie de gouvernance pour les couches et les fonctions Lambda.

Pour plus d'informations sur la AWS protection de l'infrastructure mondiale qui exécute Lambda, consultezthe section called "Sécurité de l'infrastructure".

Résilience dans AWS Lambda

L'infrastructure AWS mondiale est construite autour des AWS régions et des zones de disponibilité. AWS Les régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, qui sont connectées à un réseau à faible latence, haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone de disponibilité à l'autre sans interruption. Les zones de disponibilité sont plus hautement disponibles, tolérantes aux pannes et évolutives que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur AWS les régions et les zones de disponibilité, consultez la section Infrastructure AWS mondiale.

Outre l'infrastructure AWS mondiale, Lambda propose plusieurs fonctionnalités pour répondre à vos besoins en matière de résilience et de sauvegarde des données.

- Gestion des versions – Vous pouvez utiliser la gestion des versions dans Lambda pour enregistrer le code et la configuration de votre fonction à mesure que vous la développez. Associé aux alias, vous pouvez utiliser le versionnement pour effectuer des blue/green déploiements continus. Pour en savoir plus, consultez Gérer les versions de la fonction d'événement Lambda.
- Mise à l'échelle – Lorsque votre fonction reçoit une demande tandis qu'elle traite une demande précédente, Lambda lance une autre instance de votre fonction pour gérer la charge accrue. Lambda adapte automatiquement son échelle pour gérer 1 000 exécutions simultanées par région, un quota qui peut être augmenté si nécessaire. Pour en savoir plus, consultez Comprendre le dimensionnement des fonctions d'événement Lambda.
- Haute disponibilité – Lambda exécute votre fonction dans plusieurs zones de disponibilité afin de vous assurer qu'elle est disponible pour traiter les événements en cas d'interruption de service dans une seule zone. Si vous configurez votre fonction pour vous connecter à un cloud privé virtuel (VPC) de votre compte, spécifiez les sous-réseaux dans plusieurs zones de disponibilité, pour une garantie de haute disponibilité. Pour plus d'informations, consultez Permettre à Lambda Event Functions d'accéder aux ressources d'un Amazon VPC.
- Simultanéité réservée – Pour vous assurer que votre fonction peut toujours adapter son échelle afin de gérer des demandes supplémentaires, vous pouvez réserver de la simultanéité. La définition de la simultanéité réservée pour une fonction permet de s'assurer qu'elle peut être mise à l'échelle, sans le dépasser, un certain nombre spécifié d'appels simultanés. Cela garantit que vous ne perdez pas les demandes en raison d'autres fonctions utilisant toute la simultanéité disponible. Pour plus d'informations, consultez Configuration de la simultanéité réservée pour une fonction événementielle.
- Nouvelles tentatives – Pour les appels asynchrones et un sous-ensemble d'appels déclenchés par d'autres services, en cas d'erreur, Lambda effectue automatiquement de nouvelles tentatives espacées. Les autres clients et les Services AWS qui invoquent des fonctions de manière synchrone sont responsables de l'exécution des nouvelles tentatives. Pour en savoir plus, consultez Comprendre le comportement des nouvelles tentatives dans les fonctions d'événement Lambda.
- Dead-letter file d'attente : pour les appels asynchrones, vous pouvez configurer Lambda pour envoyer les requêtes à une file d'attente contenant des lettres mortes si toutes les nouvelles tentatives échouent. Une file d'attente de lettres mortes est une rubrique Amazon SNS ou une file d'attente Amazon SQS qui reçoit des événements en vue de leur dépannage ou d'un nouveau traitement. Pour en savoir plus, consultez Ajout d'une file d'attente de lettres mortes.

Pour plus d'informations sur le réseau et l'infrastructure physique qui protègent Lambda, consultezthe section called “Sécurité de l’infrastructure”.

Sécurité de l'infrastructure dans AWS Lambda

En tant que service géré, AWS Lambda est protégé par les procédures de sécurité du réseau mondial AWS. Pour plus d’informations sur les services de sécurité AWS et la manière dont AWS protège l’infrastructure, consultez la section Sécurité du cloud AWS. Pour concevoir votre environnement AWS en utilisant les meilleures pratiques en matière de sécurité de l’infrastructure, consultez la section Protection de l’infrastructure dans le Security Pillar AWS Well-Architected Framework (Pilier de sécurité de l’infrastructure Well-Architected Framework).

Vous utilisez les appels d'API publiés par AWS pour accéder à Lambda via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Ses suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

Sécurisation des charges de travail avec des points de terminaison publics

Pour les charges de travail accessibles au public, AWS fournit un certain nombre de fonctionnalités et de services qui peuvent contribuer à atténuer certains risques. Cette section aborde l’authentification et l’autorisation des utilisateurs de l’application ainsi que la protection des points de terminaison d’API.

Authentification et autorisation

L’authentification est liée à l’identité et l’autorisation concerne les actions. Utilisez l’authentification pour contrôler qui peut invoquer une fonction Lambda, puis utilisez l’autorisation pour contrôler qui peut faire quoi. Pour de nombreuses applications, IAM est suffisant pour gérer les deux mécanismes de contrôle.

Pour les applications utilisant des utilisateurs externes, telles que les applications Web ou mobiles, il est courant d’utiliser des jetons Web JSON (JWT) pour gérer l’authentification et l’autorisation.

Contrairement à la gestion traditionnelle des mots de passe basée sur le serveur, les JWT sont transmis par le client à chaque demande. Ils constituent un moyen cryptographiquement sécurisé de vérifier l'identité et les demandes à l'aide des données transmises par le client. Pour les Lambda-based applications, vous pouvez sécuriser chaque appel vers chaque point de terminaison d'API sans avoir à vous fier à un serveur central pour l'authentification.

Vous pouvez implémenter des JWT avec Amazon Cognito, un service de répertoire d'utilisateurs capable de gérer l'enregistrement, l'authentification, la récupération des comptes et d'autres opérations courantes de gestion des comptes. Le cadre Amplify fournit des bibliothèques pour simplifier l'intégration de ce service dans votre application frontale. Vous pouvez également envisager des services partenaires tiers comme Auth0.

Compte tenu du rôle essentiel d'un service de fournisseur d'identité en matière de sécurité, il est important d'utiliser des outils professionnels pour protéger votre application. Il n'est pas recommandé de créer vos propres services pour gérer l'authentification ou l'autorisation. Toute vulnérabilité dans les bibliothèques personnalisées peut avoir des implications importantes pour la sécurité de votre charge de travail et de ses données.

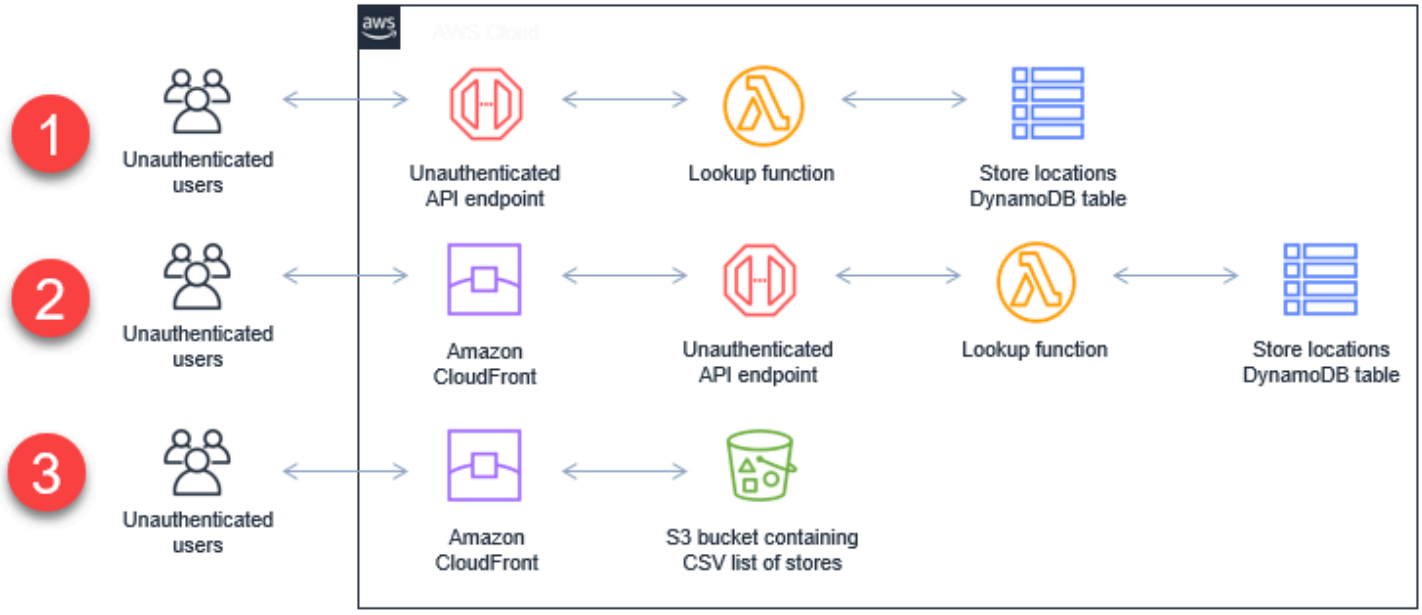
Protection des points de terminaison d'API

Pour les applications sans serveur, la méthode préférée pour servir publiquement une application dorsale consiste à utiliser Amazon API Gateway. Cela peut vous aider à protéger une API contre les utilisateurs malveillants ou les pics de trafic.

API Gateway propose deux types de points de terminaison pour les développeurs sans serveur : les API REST et les API HTTP. Les deux prennent en charge l'autorisation à AWS Lambda l'aide d'IAM ou d'Amazon Cognito. Lorsque vous utilisez IAM ou Amazon Cognito, les demandes entrantes sont évaluées et si elles ne contiennent pas le jeton requis ou si elles contiennent une authentification non valide, la demande est rejetée. Ces demandes ne vous sont pas facturées et elles ne sont pas prises en compte dans le calcul des quotas de limitation.

Les routes d'API non authentifiées sont accessibles à tous sur Internet public. Il est donc recommandé de limiter l'utilisation d'API non authentifiées. Si vous devez utiliser des API non authentifiées, il est important de les protéger contre les risques courants, tels que les attaques par déni de service (DoS). Appliquer AWS WAF à ces API peut aider à protéger votre application contre les attaques par injection SQL et par scripts inter-site (XSS). API Gateway implémente également la limitation au AWS niveau du compte et par client lorsque des clés d'API sont utilisées.

Dans de nombreux cas, les fonctionnalités fournies par une API non authentifiée peuvent être obtenues par une autre approche. Par exemple, une application Web peut fournir une liste des magasins de détail des clients à partir d'un tableau DynamoDB aux utilisateurs qui ne sont pas connectés. Cette demande peut provenir d'une application Web frontale ou de toute autre source qui appelle le point de terminaison de l'URL. Ce schéma compare trois solutions :



1. Cette API non authentifiée peut être appelée par quiconque sur Internet. Lors d'une attaque par déni de service, il est possible d'épuiser les limites de limitation des API, la simultanéité Lambda ou la capacité de lecture provisionnée par DynamoDB sur une table sous-jacente.
2. Une CloudFront distribution devant le point de terminaison de l'API avec une configuration de durée de vie (TTL) appropriée absorberait la majeure partie du trafic lors d'une attaque DoS, sans modifier la solution sous-jacente pour récupérer les données.
3. Sinon, pour les données statiques qui changent rarement, la CloudFront distribution peut diffuser les « données » provenant d'un compartiment Amazon S3.

Utilisation de la signature de code pour vérifier l'intégrité du code avec Lambda

La signature de code permet de s'assurer que seul du code approuvé est déployé dans vos fonctions Lambda. À l'aide de AWS Signer, vous pouvez créer des packages de code signés numériquement pour vos fonctions. Lorsque vous ajoutez une configuration de signature de code à une fonction, Lambda vérifie que tous les nouveaux déploiements de code sont signés par une source approuvée.

Étant donné que les contrôles de validation de signature de code s'exécutent au moment du déploiement, l'exécution de la fonction n'est aucunement affectée. Pour plus d'informations sur la gestion des politiques de signature de code, consultezthe section called "Permissions".

> **Note**
>
> La signature de code s'applique aux fonctions d'événement Lambda déployées sous forme de packages d'images .zip ou de conteneurs. Il n'est pas utilisé par Lambda Web Functions ou Lambda MicroVMS.

> **Important**
>
> Les configurations de signature de code empêchent uniquement les nouveaux déploiements de code non signé. Si vous ajoutez une configuration de signature de code à une fonction existante contenant du code non signé, ce code continue de s'exécuter jusqu'à ce que vous déployiez un nouveau package de code.

Lorsque vous activez la signature de code pour une fonction, toutes les couches que vous ajoutez à la fonction doivent également être signées par un profil de signature autorisé.

Il n'y a aucun frais supplémentaire pour l'utilisation AWS Signer ou la signature de code pour AWS Lambda.

Validation de signature

Lambda effectue les contrôles de validation suivants lorsque vous déployez un package de code signé vers votre fonction :

1. Intégrité : vérifie que le package de code n'a pas été modifié depuis sa signature. Lambda compare le hachage du package au hachage de la signature.
2. Expiration : affirme que la signature du package de code n'a pas expiré.
3. Incompatibilité : affirme que le package de code est signé avec un profil de signature autorisé
4. Révocation : affirme que la signature du package de code n'a pas été révoquée.

Lorsque vous créez une configuration de signature de code, vous pouvez utiliser le UntrustedArtifactOnDeploymentparamètre pour spécifier la manière dont Lambda doit réagir en cas

d'échec des contrôles d'expiration, d'incompatibilité ou de révocation. Vous pouvez choisir l'une de ces actions :

- `Warn` : il s'agit du paramètre par défaut. Lambda autorise le déploiement du package de code, mais émet un avertissement. Lambda émet une nouvelle CloudWatch métrique Amazon (`SignatureValidationErrors`) et enregistre également l'avertissement dans le CloudTrail journal.
- `Enforce` : Lambda émet un avertissement (identique à celui de l'action `Warn`) et bloque le déploiement du package de code.

Rubriques

- Création de configurations de signature de code pour Lambda
- Configuration des politiques IAM pour les configurations de signature de code Lambda
- Utilisation des balises dans les configurations de signature de code

Création de configurations de signature de code pour Lambda

Afin d'activer la signature de code pour une fonction, vous créez une configuration de signature de code et l'attachez à la fonction. Une configuration de signature de code définit une liste de profils de signature autorisés et l'action de stratégie à privilégier en cas d'échec de l'un des contrôles de validation.

> **Note**
>
> Les fonctions définies en tant qu'images de conteneur ne prennent pas en charge la signature de code.

Sections

- Conditions préalables à la configuration
- Création de configurations de signature de code
- Activation de la signature de code pour une fonction

Conditions préalables à la configuration

Avant de configurer la signature de code pour une fonction Lambda, utilisez AWS Signer pour effectuer les opérations suivantes :

- Créer un ou plusieurs profils de signature.
- Utiliser un profil de signature afin de créer un package de code signé pour votre fonction.

Création de configurations de signature de code

Une configuration de signature de code définit une liste des profils de signature autorisés et la stratégie de validation de signature.

Pour créer une configuration de signature de code (console)

1. Ouvrez la page des configurations de signature de code de la console Lambda.
2. Choisissez Créer une configuration.
3. Pour Description, saisissez un nom descriptif pour la configuration.
4. Sous Signing profiles (Profils de signature), ajoutez jusqu'à 20 profils de signature à la configuration.
    a. Pour Signing profile version ARN (ARN de la version du profil de signature), sélectionnez l'Amazon Resource Name (ARN) de la version du profil, ou saisissez l'ARN.
    b. Pour ajouter un profil de signature supplémentaire, sélectionnez Add signing profiles (Ajouter des profils de signature).
5. Sous Signature validation policy (Stratégie de validation de signature), sélectionnez Warn (Avertissement) ou Enforce (Application).
6. Choisissez Créer une configuration.

Activation de la signature de code pour une fonction

Afin d’activer la signature de code pour une fonction, ajoutez une configuration de signature de code à la fonction.

> **Important**
>
> Les configurations de signature de code empêchent uniquement les nouveaux déploiements de code non signé. Si vous ajoutez une configuration de signature de code à une fonction existante contenant du code non signé, ce code continue de s'exécuter jusqu'à ce que vous déployiez un nouveau package de code.

Pour associer une configuration de signature de code à une fonction (console)

1. Ouvrez la page Event Functions de la console Lambda.
2. Sélectionnez la fonction pour laquelle vous souhaitez activer la signature de code.
3. Ouvrez l'onglet Configuration.
4. Faites défiler vers le bas et choisissez Signature de code.
5. Choisissez Modifier.
6. Sous Edit code signing (Modifier la signature de code), sélectionnez une configuration de signature de code pour cette fonction.
7. Choisissez Enregistrer.

Configuration des politiques IAM pour les configurations de signature de code Lambda

Pour accorder à un utilisateur l'autorisation d'accéder aux opérations d'API de signature de code Lambda, attachez une ou plusieurs instructions de stratégie à la stratégie utilisateur. Pour plus d'informations sur les stratégies utilisateur, consultez Identity-based Politiques IAM pour Lambda.

L'exemple d'instruction de stratégie suivant autorise la création, la mise à jour et la récupération de configurations de signature de code.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
```

```
      "Effect": "Allow",
      "Action": [
          "lambda:CreateCodeSigningConfig",
          "lambda:UpdateCodeSigningConfig",
          "lambda:GetCodeSigningConfig"
        ],
      "Resource": "*"
    }
  ]
}
```

Les administrateurs peuvent utiliser la clé de condition `CodeSigningConfigArn` pour spécifier les configurations de signature de code que les développeurs doivent utiliser pour créer ou mettre à jour vos fonctions.

L'exemple de déclaration de stratégie suivant accorde l'autorisation de créer une fonction. La déclaration de stratégie comprend une condition `lambda:CodeSigningConfigArn` pour spécifier la configuration de signature de code autorisée. Lambda bloque les demandes `CreateFunction` d'API si le CodeSigningConfigArnparamètre est absent ou ne correspond pas à la valeur de la condition.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "AllowReferencingCodeSigningConfig",
      "Effect": "Allow",
      "Action": [
        "lambda:CreateFunction"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "lambda:CodeSigningConfigArn": "arn:aws:lambda:us-
east-1:111122223333:code-signing-config:csc-0d4518bd353a0a7c6"
        }
      }
    }
  ]
```

```
}
```

Utilisation des balises dans les configurations de signature de code

Vous pouvez étiqueter les configurations de signature de code pour organiser et gérer vos ressources. Les balises sont des paires clé-valeur de forme libre associées à vos ressources prises en charge par l'ensemble des ressources Services AWS. Pour plus d'informations sur les cas d'utilisation des balises, consultez la section Stratégies de balisage courantes dans le guide des AWS ressources de balisage et de l'éditeur de balises.

Vous pouvez utiliser l' AWS Lambda API pour afficher et mettre à jour les balises. Vous pouvez également afficher et mettre à jour les balises tout en gérant une configuration de signature de code spécifique dans la console Lambda.

Sections

- Autorisations requises pour l'utilisation des balises
- Utilisation des balises avec la console Lambda
- Utilisation de balises avec le AWS CLI

Autorisations requises pour l'utilisation des balises

Pour autoriser une identité Gestion des identités et des accès AWS (IAM) – utilisateur, groupe ou rôle – à afficher ou marquer les ressources, accordez-lui les autorisations correspondantes :

- lambda : ListTags —Lorsqu' une ressource possède des balises, accordez cette autorisation à tous ceux qui ont besoin de `ListTags` l'utiliser. Pour les fonctions d'événement balisées, cette autorisation est également nécessaire pour`GetFunction`.
- lambda : TagResource —Accordez cette autorisation à toute personne ayant besoin d'appeler `TagResource` ou d'exécuter un tag lors de la création.

Vous pouvez éventuellement envisager d'accorder également l'UntagResourceautorisation lambda : pour autoriser les `UntagResource` appels à la ressource.

Pour plus d'informations, consultez Identity-based Politiques IAM pour Lambda.

Utilisation des balises avec la console Lambda

Vous pouvez utiliser la console Lambda pour créer des configurations de signature de code qui comportent des balises, pour ajouter des balises aux configurations de signature de code existantes et pour filtrer des configurations de signature de code par balise.

Ajout d'une balise lors de la création d'une configuration de signature de code

1. Ouvrez la page Configurations de signature de code dans la console Lambda.
2. Dans l'en-tête du volet de contenu, choisissez Créer une configuration.
3. Dans la section située en haut du volet de contenu, configurez votre signature de code. Pour plus d'informations sur la configuration des configurations de signature de code, consultez the section called "Signature de code".
4. Dans la section Balises, choisissez Ajouter une balise.
5. Dans le champ Clé, saisissez la clé de votre balise. Pour plus d'informations sur les restrictions relatives au balisage, consultez la section Limites et exigences relatives au nommage des balises dans le Guide des AWS ressources de balisage et de l'éditeur de balises.
6. Choisissez Créer une configuration.

Pour ajouter une balise à une configuration de signature de code existante

1. Ouvrez la page Configurations de signature de code dans la console Lambda.
2. Sélectionnez le nom de votre configuration de signature de code.
3. Dans les onglets situés sous le volet Détails, sélectionnez Balises.
4. Choisissez Gérer les balises.
5. Choisissez Add new tag (Ajouter une nouvelle balise).
6. Dans le champ Clé, saisissez la clé de votre balise. Pour plus d'informations sur les restrictions relatives au balisage, consultez la section Limites et exigences relatives au nommage des balises dans le Guide des AWS ressources de balisage et de l'éditeur de balises.
7. Cliquez sur Enregistrer.

Pour filtrer les configurations de signature de code par balise

1. Ouvrez la page Configurations de signature de code dans la console Lambda.

2. Cliquez sur la barre de recherche.
3. Dans la liste déroulante, sélectionnez votre balise sous le sous-titre Balises.
4. Sélectionnez Utiliser : « tag-name » pour afficher toutes les configurations de signature de code étiquetées avec cette touche, ou choisissez un Opérateur pour affiner le filtrage en fonction de la valeur.
5. Sélectionnez votre valeur de balise pour appliquer un filtre combinant la clé et la valeur de la balise.

La zone de recherche prend également en charge la recherche de clés de balise. Saisissez le nom d'une clé pour la rechercher dans la liste.

Utilisation de balises avec le AWS CLI

Vous pouvez ajouter et supprimer des balises sur les ressources Lambda existantes, configurations de signature de code incluses, avec l'API Lambda. Vous pouvez également ajouter des balises lors de la création d'une configuration de signature de code afin de maintenir une ressource étiquetée tout au long de son cycle de vie.

Mise à jour des balises avec les API de balises Lambda

Vous pouvez ajouter et supprimer des balises pour les ressources Lambda prises en charge par le biais des opérations TagResourceet de l'UntagResourceAPI.

Vous pouvez appeler ces opérations par l'intermédiaire de l' AWS CLI. Pour ajouter des balises à une ressource existante, utilisez la commande `tag-resource`. Cet exemple ajoute deux balises, l'une avec la clé *`Department`* et l'autre avec la clé*`CostCenter`*.

```
aws lambda tag-resource \
--resource arn:aws:lambda:us-east-2:123456789012:resource-type:my-resource \
--tags Department=Marketing,CostCenter=1234ABCD
```

Pour supprimer des balises, utilisez la commande `untag-resource`. Cet exemple supprime la balise contenant la clé*`Department`*.

```
aws lambda untag-resource --resource arn:aws:lambda:us-east-1:123456789012:resource-
type:resource-identifier \
--tag-keys Department
```

Ajout de balises lors de la création d'une configuration de signature de code

Pour créer une nouvelle configuration de signature de code Lambda avec des balises, utilisez l'opération CreateCodeSigningConfigAPI. Spécifiez le paramètre `Tags`. Vous pouvez appeler cette opération à l'aide de la `create-code-signing-config` AWS CLI commande et de l'`--tags`option. Pour plus d'informations sur la commande de la CLI, consultez create-code-signing-config dans la Référence des commandes de l'AWS CLI .

Avant d'utiliser le paramètre `Tags` avec `CreateCodeSigningConfig`, vérifiez que votre rôle dispose de l'autorisation d'étiqueter les ressources en plus des autorisations habituelles nécessaires à cette opération. Pour plus d'informations sur les autorisations requises pour l'étiquetage, consultez the section called "Autorisations requises pour l'utilisation des balises".

Affichage des balises avec les API de balises Lambda

Pour afficher les balises associées à une ressource Lambda spécifique, utilisez l'opération d'API `ListTags`. Pour plus d'informations, consultez ListTags.

Vous pouvez appeler cette opération à l'aide de la `list-tags` AWS CLI commande en fournissant un ARN (Amazon Resource Name).

```
aws lambda list-tags --resource arn:aws:lambda:us-east-1:123456789012:resource-type:resource-identifier
```

Filtrage de ressources par balise

Vous pouvez utiliser l'opération AWS Resource Groups Tagging API GetResourcesAPI pour filtrer vos ressources par balises. L'opération `GetResources` reçoit jusqu'à 10 filtres, chaque filtre contenant une clé de balise et jusqu'à 10 valeurs de balise. Vous fournissez `GetResources`avec un `ResourceType` pour filtrer par certains types de ressources.

Vous pouvez appeler cette opération à l'aide de la `get-resources` AWS CLI commande. Pour des exemples d'utilisation de `get-resources`, consultez get-resources dans la Référence des commandes de l'AWS CLI.

Utilisation de Lambda avec un AWS Kit SDK

AWS des kits de développement logiciel (SDK) sont disponibles pour de nombreux langages de programmation courants. Chaque kit SDK fournit une API, des exemples de code et de la documentation qui facilitent la création d'applications par les développeurs dans leur langage préféré.

Documentation SDK	Exemples de code
AWS SDK pour C++	AWS SDK pour C++ exemples de code
AWS CLI	AWS CLI exemples de code
AWS SDK pour Go	AWS SDK pour Go exemples de code
AWS SDK pour Java	AWS SDK pour Java exemples de code
AWS SDK pour JavaScript	AWS SDK pour JavaScript exemples de code
AWS SDK pour Kotlin	AWS SDK pour Kotlin exemples de code
AWS SDK pour .NET	AWS SDK pour .NET exemples de code
AWS SDK pour PHP	AWS SDK pour PHP exemples de code
Outils AWS pour PowerShell	Outils AWS pour PowerShell exemples de code
AWS SDK pour Python v4	AWS Exemples de code du SDK pour Python v4
AWS SDK pour Python (Boto3)	AWS SDK pour Python (Boto3) exemples de code
AWS SDK pour Ruby	AWS SDK pour Ruby exemples de code
AWS SDK pour Rust	AWS SDK pour Rust exemples de code
AWS SDK pour SAP ABAP	AWS SDK pour SAP ABAP exemples de code
AWS SDK pour Swift	AWS SDK pour Swift exemples de code

Pour plus d'exemples spécifiques à Lambda, consultez Exemples de code pour Lambda utilisant AWS Kits SDK.

> **Exemple de disponibilité**
>
> Vous n’avez pas trouvé ce dont vous avez besoin ? Demandez un exemple de code en utilisant le lien Provide feedback (Fournir un commentaire) en bas de cette page.

Exemples de code pour Lambda utilisant AWS Kits SDK

Les exemples de code suivants montrent comment utiliser Lambda avec un AWS kit de développement logiciel (SDK).

Les principes de base sont des exemples de code qui vous montrent comment effectuer les opérations essentielles au sein d'un service.

Les actions sont des extraits de code de programmes plus larges et doivent être exécutées dans leur contexte. Alors que les actions vous indiquent comment appeler des fonctions de service individuelles, vous pouvez les voir en contexte dans leurs scénarios associés.

Les scénarios sont des exemples de code qui vous montrent comment accomplir des tâches spécifiques en appelant plusieurs fonctions au sein d'un même service ou combinés à d'autres Services AWS.

AWS contributions communautaires sont des exemples qui ont été créés et sont gérés par plusieurs équipes à travers AWS. Pour faire un commentaire, utilisez le mécanisme fourni dans les référentiels liés.

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Exemples de code utilisant le SDK

- Exemples basiques d'utilisation de Lambda AWS Kits SDK
  - Hello Lambda
  - Apprenez les bases de Lambda avec AWS Kit SDK
  - Actions pour Lambda à l'aide de AWS Kits SDK
    - Utilisation de CreateAlias avec une CLI
    - Utiliser CreateFunction avec un AWS SDK ou CLI
    - Utilisation de DeleteAlias avec une CLI
    - Utiliser DeleteFunction avec un AWS SDK ou CLI
    - Utilisation de DeleteFunctionConcurrency avec une CLI
    - Utilisation de DeleteProvisionedConcurrencyConfig avec une CLI
    - Utilisation de GetAccountSettings avec une CLI

- Utilisation de GetAlias avec une CLI
- Utiliser GetFunction avec un AWS SDK ou CLI
- Utilisation de GetFunctionConcurrency avec une CLI
- Utilisation de GetFunctionConfiguration avec une CLI
- Utilisation de GetPolicy avec une CLI
- Utilisation de GetProvisionedConcurrencyConfig avec une CLI
- Utiliser Invoquer avec un AWS SDK ou CLI
- Utiliser ListFunctions avec un AWS SDK ou CLI
- Utilisation de ListProvisionedConcurrencyConfigs avec une CLI
- Utilisation de ListTags avec une CLI
- Utilisation de ListVersionsByFunction avec une CLI
- Utilisation de PublishVersion avec une CLI
- Utilisation de PutFunctionConcurrency avec une CLI
- Utilisation de PutProvisionedConcurrencyConfig avec une CLI
- Utilisation de RemovePermission avec une CLI
- Utilisation de TagResource avec une CLI
- Utilisation de UntagResource avec une CLI
- Utilisation de UpdateAlias avec une CLI
- Utiliser UpdateFunctionCode avec un AWS SDK ou CLI
- Utiliser UpdateFunctionConfiguration avec un AWS SDK ou CLI

- Scénarios pour Lambda utilisant AWS Kits SDK
  - Confirmez automatiquement les utilisateurs connus d'Amazon Cognito à l'aide d'une fonction Lambda à l'aide d'un AWS Kit SDK
  - Migrez automatiquement les utilisateurs connus d'Amazon Cognito à l'aide d'une fonction Lambda à l'aide d'un AWS Kit SDK
  - Créez une API REST API Gateway pour effectuer le suivi COVID-19 données
  - Créer une API REST de bibliothèque de prêt
  - Créer une application de messagerie avec Step Functions
  - Création d'une API REST avec intégration de fonctions proxy
  - Création d’une application de gestion des ressources photographiques permettant aux utilisateurs de gérer les photos à l’aide d’étiquettes

- Créer une application de chat Websocket avec API Gateway
- Créez une application qui analyse les commentaires des clients et synthétise le son
- Création d'un tableau de bord de surveillance avec le nom de fonction comme variable
- Création de votre première fonction sans serveur
- Invoquer une fonction Lambda à partir d'un navigateur
- Transformation des données pour votre application avec S3 Object Lambda
- Utiliser API Gateway pour invoquer une fonction Lambda
- Utiliser les fonctions Step Functions pour invoquer des fonctions Lambda
- Utilisent des événements planifiés pour invoquer une fonction Lambda
- Utiliser l'API Amazon Neptune pour développer une fonction Lambda qui interroge les données d'un graphe
- Utilisation de variables de propriété dans les tableaux de bord de surveillance pour surveiller plusieurs fonctions sans serveur
- Écrivez des données d'activité personnalisées à l'aide d'une fonction Lambda après l'authentification utilisateur Amazon Cognito à l'aide d'un AWS Kit SDK

- Exemples sans serveur pour Lambda
  - Connexion à une base de données Amazon RDS dans une fonction Lambda
  - Invoquer une fonction Lambda à partir d'un déclencheur Kinesis
  - Invocation d'une fonction Lambda à partir d'un déclencheur DynamoDB
  - Invocation d'une fonction Lambda à partir d'un déclencheur Amazon DocumentDB
  - Invocation d'une fonction Lambda à partir d'un déclencheur Amazon MSK
  - Invoquer une fonction Lambda à partir d'un déclencheur Amazon S3
  - Invocation d'une fonction lambda à partir d'un déclencheur Amazon SNS
  - Invoquer une fonction Lambda à partir d'un déclencheur Amazon SQS
  - Signalement des échecs d'articles par lots pour les fonctions Lambda à l'aide d'un déclencheur Kinesis
  - Signalement des échecs d'articles par lots pour les fonctions Lambda à l'aide d'un déclencheur DynamoDB
  - Signalement des échecs d'articles par lots pour les fonctions Lambda à l'aide d'un déclencheur Amazon SQS
- AWS contributions de la communauté pour Lambda

- Création et test d'une application sans serveur

Exemples basiques d'utilisation de Lambda AWS Kits SDK

Les exemples de code suivants montrent comment utiliser les bases de AWS Lambda avec AWS SDK.

Exemples

- Hello Lambda
- Apprenez les bases de Lambda avec AWS Kit SDK
- Actions pour Lambda à l'aide de AWS Kits SDK
  - Utilisation de CreateAlias avec une CLI
  - Utiliser CreateFunction avec un AWS SDK ou CLI
  - Utilisation de DeleteAlias avec une CLI
  - Utiliser DeleteFunction avec un AWS SDK ou CLI
  - Utilisation de DeleteFunctionConcurrency avec une CLI
  - Utilisation de DeleteProvisionedConcurrencyConfig avec une CLI
  - Utilisation de GetAccountSettings avec une CLI
  - Utilisation de GetAlias avec une CLI
  - Utiliser GetFunction avec un AWS SDK ou CLI
  - Utilisation de GetFunctionConcurrency avec une CLI
  - Utilisation de GetFunctionConfiguration avec une CLI
  - Utilisation de GetPolicy avec une CLI
  - Utilisation de GetProvisionedConcurrencyConfig avec une CLI
  - Utiliser Invoquer avec un AWS SDK ou CLI
  - Utiliser ListFunctions avec un AWS SDK ou CLI
  - Utilisation de ListProvisionedConcurrencyConfigs avec une CLI
  - Utilisation de ListTags avec une CLI
  - Utilisation de ListVersionsByFunction avec une CLI
  - Utilisation de PublishVersion avec une CLI
  - Utilisation de PutFunctionConcurrency avec une CLI

- Utilisation de PutProvisionedConcurrencyConfig avec une CLI
- Utilisation de RemovePermission avec une CLI
- Utilisation de TagResource avec une CLI
- Utilisation de UntagResource avec une CLI
- Utilisation de UpdateAlias avec une CLI
- Utiliser UpdateFunctionCode avec un AWS SDK ou CLI
- Utiliser UpdateFunctionConfiguration avec un AWS SDK ou CLI

Hello Lambda

Les exemples de code suivants montrent comment démarrer avec Lambda.

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
namespace LambdaActions;

using Amazon.Lambda;

public class HelloLambda
{
    static async Task Main(string[] args)
    {
        var lambdaClient = new AmazonLambdaClient();

        Console.WriteLine("Hello AWS Lambda");
        Console.WriteLine("Let's get started with AWS Lambda by listing your
 existing Lambda functions:");

        var response = await lambdaClient.ListFunctionsAsync();
        response.Functions.ForEach(function =>
        {
```

```
 Console.WriteLine($"{function.FunctionName}\t{function.Description}");
        });
    }
}
```

- Pour plus de détails sur l'API, voir ListFunctions dans AWS SDK pour .NET Référence d'API.

C++

SDK pour C++

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Code pour le CMakeLists.txt Fichier CMake.

```
# Set the minimum required version of CMake for this project.
cmake_minimum_required(VERSION 3.13)

# Set the AWS service components used by this project.
set(SERVICE_COMPONENTS lambda)

# Set this project's name.
project("hello_lambda")

# Set the C++ standard to use to build this target.
# At least C++ 11 is required for the AWS SDK for C++.
set(CMAKE_CXX_STANDARD 11)

# Use the MSVC variable to determine if this is a Windows build.
set(WINDOWS_BUILD ${MSVC})

if (WINDOWS_BUILD) # Set the location where CMake can find the installed
 libraries for the AWS SDK.
```

```
    string(REPLACE ";" "/aws-cpp-sdk-all;" SYSTEM_MODULE_PATH
 "${CMAKE_SYSTEM_PREFIX_PATH}/aws-cpp-sdk-all")
    list(APPEND CMAKE_PREFIX_PATH ${SYSTEM_MODULE_PATH})
endif ()

# Find the AWS SDK for C++ package.
find_package(AWSSDK REQUIRED COMPONENTS ${SERVICE_COMPONENTS})

if (WINDOWS_BUILD AND AWSSDK_INSTALL_AS_SHARED_LIBS)
     # Copy relevant AWS SDK for C++ libraries into the current binary directory
 for running and debugging.

     # set(BIN_SUB_DIR "/Debug") # if you are building from the command line you
 may need to uncomment this
                                    # and set the proper subdirectory to the
 executables' location.

     AWSSDK_CPY_DYN_LIBS(SERVICE_COMPONENTS ""
 ${CMAKE_CURRENT_BINARY_DIR}${BIN_SUB_DIR})
endif ()

add_executable(${PROJECT_NAME}
        hello_lambda.cpp)

target_link_libraries(${PROJECT_NAME}
        ${AWSSDK_LINK_LIBRARIES})
```

Code pour le fichier source hello_lambda.cpp.

```
#include <aws/core/Aws.h>
#include <aws/lambda/LambdaClient.h>
#include <aws/lambda/model/ListFunctionsRequest.h>
#include <iostream>

/*
 *  A "Hello Lambda" starter application which initializes an AWS Lambda (Lambda)
 client and lists the Lambda functions.
 *
 *  main function
 *
 *  Usage: 'hello_lambda'
 *
```

```
 */

int main(int argc, char **argv) {
    Aws::SDKOptions options;
    // Optionally change the log level for debugging.
//   options.loggingOptions.logLevel = Utils::Logging::LogLevel::Debug;
    Aws::InitAPI(options); // Should only be called once.
    int result = 0;
    {
        Aws::Client::ClientConfiguration clientConfig;
        // Optional: Set to the AWS Region (overrides config file).
        // clientConfig.region = "us-east-1";

        Aws::Lambda::LambdaClient lambdaClient(clientConfig);
        std::vector<Aws::String> functions;
        Aws::String marker; // Used for pagination.

        do {
            Aws::Lambda::Model::ListFunctionsRequest request;
            if (!marker.empty()) {
                request.SetMarker(marker);
            }

            Aws::Lambda::Model::ListFunctionsOutcome outcome =
 lambdaClient.ListFunctions(
                    request);

            if (outcome.IsSuccess()) {
                const Aws::Lambda::Model::ListFunctionsResult
 &listFunctionsResult = outcome.GetResult();
                std::cout << listFunctionsResult.GetFunctions().size()
                          << " lambda functions were retrieved." << std::endl;

                for (const Aws::Lambda::Model::FunctionConfiguration
 &functionConfiguration: listFunctionsResult.GetFunctions()) {
                    functions.push_back(functionConfiguration.GetFunctionName());
                    std::cout << functions.size() << "  "
                              << functionConfiguration.GetDescription() <<
 std::endl;
                    std::cout << "   "
                              <<
 Aws::Lambda::Model::RuntimeMapper::GetNameForRuntime(
                                      functionConfiguration.GetRuntime()) << ": "
                              << functionConfiguration.GetHandler()
```

```
                                << std::endl;
                }
                marker = listFunctionsResult.GetNextMarker();
            } else {
                std::cerr << "Error with Lambda::ListFunctions. "
                          << outcome.GetError().GetMessage()
                          << std::endl;
                result = 1;
                break;
            }
        } while (!marker.empty());
    }


    Aws::ShutdownAPI(options); // Should only be called once.
    return result;
}
```

- Pour plus de détails sur l'API, voir ListFunctions dans AWS SDK pour C++ Référence d'API.

Go

Kit SDK pour Go V2

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
package main

import (
 "context"
 "fmt"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/config"
 "github.com/aws/aws-sdk-go-v2/service/lambda"
)
```

```
// main uses the AWS SDK for Go (v2) to create an AWS Lambda client and list up
 to 10
// functions in your account.
// This example uses the default settings specified in your shared credentials
// and config files.
func main() {
 ctx := context.Background()
 sdkConfig, err := config.LoadDefaultConfig(ctx)
 if err != nil {
  fmt.Println("Couldn't load default configuration. Have you set up your AWS
 account?")
  fmt.Println(err)
  return
 }
 lambdaClient := lambda.NewFromConfig(sdkConfig)

 maxItems := 10
 fmt.Printf("Let's list up to %v functions for your account.\n", maxItems)
 result, err := lambdaClient.ListFunctions(ctx, &lambda.ListFunctionsInput{
  MaxItems: aws.Int32(int32(maxItems)),
 })
 if err != nil {
  fmt.Printf("Couldn't list functions for your account. Here's why: %v\n", err)
  return
 }
 if len(result.Functions) == 0 {
  fmt.Println("You don't have any functions!")
 } else {
  for _, function := range result.Functions {
   fmt.Printf("\t%v\n", *function.FunctionName)
  }
 }
}
```

- Pour plus de détails sur l'API, voir ListFunctions dans AWS SDK pour Go Référence d'API.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    /**
     * Lists the AWS Lambda functions associated with the current AWS account.
     *
     * @param awsLambda an instance of the {@link LambdaClient} class, which is
used to interact with the AWS Lambda service
     *
     * @throws LambdaException if an error occurs while interacting with the AWS
Lambda service
     */
    public static void listFunctions(LambdaClient awsLambda) {
        try {
            ListFunctionsResponse functionResult = awsLambda.listFunctions();
            List<FunctionConfiguration> list = functionResult.functions();
            for (FunctionConfiguration config : list) {
                System.out.println("The function name is " +
config.functionName());
            }

        } catch (LambdaException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
```

- Pour plus de détails sur l'API, voir ListFunctions dans AWS SDK for Java 2.x Référence d'API.

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import { LambdaClient, paginateListFunctions } from "@aws-sdk/client-lambda";

const client = new LambdaClient({});

export const helloLambda = async () => {
  const paginator = paginateListFunctions({ client }, {});
  const functions = [];

  for await (const page of paginator) {
    const funcNames = page.Functions.map((f) => f.FunctionName);
    functions.push(...funcNames);
  }

  console.log("Functions:");
  console.log(functions.join("\n"));
  return functions;
};
```

- Pour plus de détails sur l'API, voir ListFunctions dans AWS SDK pour JavaScript Référence d'API.

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import boto3


def main():
    """
    List the Lambda functions in your AWS account.
    """
    # Create the Lambda client
    lambda_client = boto3.client("lambda")

    # Use the paginator to list the functions
    paginator = lambda_client.get_paginator("list_functions")
    response_iterator = paginator.paginate()

    print("Here are the Lambda functions in your account:")
    for page in response_iterator:
        for function in page["Functions"]:
            print(f"  {function['FunctionName']}")


if __name__ == "__main__":
    main()
```

- Pour plus de détails sur l'API, voir ListFunctions dans AWS Référence de l'API du SDK pour Python (Boto3).

Ruby

Kit SDK pour Ruby

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
require 'aws-sdk-lambda'
```

```
# Creates an AWS Lambda client using the default credentials and configuration
def lambda_client
  Aws::Lambda::Client.new
end

# Lists the Lambda functions in your AWS account, paginating the results if
 necessary
def list_lambda_functions
  lambda = lambda_client

  # Use a pagination iterator to list all functions
  functions = []
  lambda.list_functions.each_page do |page|
    functions.concat(page.functions)
  end

  # Print the name and ARN of each function
  functions.each do |function|
    puts "Function name: #{function.function_name}"
    puts "Function ARN: #{function.function_arn}"
    puts
  end

  puts "Total functions: #{functions.count}"
end

list_lambda_functions if __FILE__ == $PROGRAM_NAME
```

- Pour plus de détails sur l'API, voir ListFunctions dans AWS SDK pour Ruby Référence d'API.

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Apprenez les bases de Lambda avec AWS Kit SDK

Les exemples de code suivants montrent comment :

- Créer un rôle IAM et une fonction Lambda, puis charger le code du gestionnaire.
- Invoquer la fonction avec un seul paramètre et obtenir des résultats.
- Mettre à jour le code de la fonction et configurer avec une variable d'environnement.
- Invoquer la fonction avec de nouveaux paramètres et obtenir des résultats. Afficher le journal d'exécution renvoyé.
- Répertorier les fonctions pour votre compte, puis nettoyer les ressources.

Pour plus d'informations, consultez Créer une fonction Lambda à l'aide de la console.

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Créez des méthodes qui exécutent des actions Lambda.

```
namespace LambdaActions;

using Amazon.Lambda;
using Amazon.Lambda.Model;

/// <summary>
/// A class that implements AWS Lambda methods.
/// </summary>
public class LambdaWrapper
{
    private readonly IAmazonLambda _lambdaService;

    /// <summary>
    /// Constructor for the LambdaWrapper class.
    /// </summary>
    /// <param name="lambdaService">An initialized Lambda service client.</param>
    public LambdaWrapper(IAmazonLambda lambdaService)
    {
        _lambdaService = lambdaService;
```

```
    }

    /// <summary>
    /// Creates a new Lambda function.
    /// </summary>
    /// <param name="functionName">The name of the function.</param>
    /// <param name="s3Bucket">The Amazon Simple Storage Service (Amazon S3)
    /// bucket where the zip file containing the code is located.</param>
    /// <param name="s3Key">The Amazon S3 key of the zip file.</param>
    /// <param name="role">The Amazon Resource Name (ARN) of a role with the
    /// appropriate Lambda permissions.</param>
    /// <param name="handler">The name of the handler function.</param>
    /// <returns>The Amazon Resource Name (ARN) of the newly created
    /// Lambda function.</returns>
    public async Task<string> CreateLambdaFunctionAsync(
        string functionName,
        string s3Bucket,
        string s3Key,
        string role,
        string handler)
    {
        // Defines the location for the function code.
        // S3Bucket - The S3 bucket where the file containing
        //            the source code is stored.
        // S3Key    - The name of the file containing the code.
        var functionCode = new FunctionCode
        {
            S3Bucket = s3Bucket,
            S3Key = s3Key,
        };

        var createFunctionRequest = new CreateFunctionRequest
        {
            FunctionName = functionName,
            Description = "Created by the Lambda .NET API",
            Code = functionCode,
            Handler = handler,
            Runtime = Runtime.Dotnet6,
            Role = role,
        };

        var reponse = await
_lambdaService.CreateFunctionAsync(createFunctionRequest);
        return reponse.FunctionArn;
```

```
    }


    /// <summary>
    /// Delete an AWS Lambda function.
    /// </summary>
    /// <param name="functionName">The name of the Lambda function to
    /// delete.</param>
    /// <returns>A Boolean value that indicates the success of the action.</
returns>
    public async Task<bool> DeleteFunctionAsync(string functionName)
    {
        var request = new DeleteFunctionRequest
        {
            FunctionName = functionName,
        };

        var response = await _lambdaService.DeleteFunctionAsync(request);

        // A return value of NoContent means that the request was processed.
        // In this case, the function was deleted, and the return value
        // is intentionally blank.
        return response.HttpStatusCode == System.Net.HttpStatusCode.NoContent;
    }


    /// <summary>
    /// Gets information about a Lambda function.
    /// </summary>
    /// <param name="functionName">The name of the Lambda function for
    /// which to retrieve information.</param>
    /// <returns>Async Task.</returns>
    public async Task<FunctionConfiguration> GetFunctionAsync(string
 functionName)
    {
        var functionRequest = new GetFunctionRequest
        {
            FunctionName = functionName,
        };

        var response = await _lambdaService.GetFunctionAsync(functionRequest);
        return response.Configuration;
    }
```

```
    /// <summary>
    /// Invoke a Lambda function.
    /// </summary>
    /// <param name="functionName">The name of the Lambda function to
    /// invoke.</param
    /// <param name="parameters">The parameter values that will be passed to the
function.</param>
    /// <returns>A System Threading Task.</returns>
    public async Task<string> InvokeFunctionAsync(
        string functionName,
        string parameters)
    {
        var payload = parameters;
        var request = new InvokeRequest
        {
            FunctionName = functionName,
            Payload = payload,
        };

        var response = await _lambdaService.InvokeAsync(request);
        MemoryStream stream = response.Payload;
        string returnValue =
System.Text.Encoding.UTF8.GetString(stream.ToArray());
        return returnValue;
    }


    /// <summary>
    /// Get a list of Lambda functions.
    /// </summary>
    /// <returns>A list of FunctionConfiguration objects.</returns>
    public async Task<List<FunctionConfiguration>> ListFunctionsAsync()
    {
        var functionList = new List<FunctionConfiguration>();

        var functionPaginator =
            _lambdaService.Paginators.ListFunctions(new ListFunctionsRequest());
        await foreach (var function in functionPaginator.Functions)
        {
            functionList.Add(function);
        }

        return functionList;
```

```
    }


    /// <summary>
    /// Update an existing Lambda function.
    /// </summary>
    /// <param name="functionName">The name of the Lambda function to update.</
param>
    /// <param name="bucketName">The bucket where the zip file containing
    /// the Lambda function code is stored.</param>
    /// <param name="key">The key name of the source code file.</param>
    /// <returns>Async Task.</returns>
    public async Task UpdateFunctionCodeAsync(
        string functionName,
        string bucketName,
        string key)
    {
        var functionCodeRequest = new UpdateFunctionCodeRequest
        {
            FunctionName = functionName,
            Publish = true,
            S3Bucket = bucketName,
            S3Key = key,
        };

        var response = await
 _lambdaService.UpdateFunctionCodeAsync(functionCodeRequest);
       Console.WriteLine($"The Function was last modified at
 {response.LastModified}.");
    }


    /// <summary>
    /// Update the code of a Lambda function.
    /// </summary>
    /// <param name="functionName">The name of the function to update.</param>
    /// <param name="functionHandler">The code that performs the function's
 actions.</param>
    /// <param name="environmentVariables">A dictionary of environment
 variables.</param>
    /// <returns>A Boolean value indicating the success of the action.</returns>
    public async Task<bool> UpdateFunctionConfigurationAsync(
        string functionName,
        string functionHandler,
```

```
        Dictionary<string, string> environmentVariables)
    {
        var request = new UpdateFunctionConfigurationRequest
        {
            Handler = functionHandler,
            FunctionName = functionName,
            Environment = new Amazon.Lambda.Model.Environment { Variables =
 environmentVariables },
        };

        var response = await
 _lambdaService.UpdateFunctionConfigurationAsync(request);

        Console.WriteLine(response.LastModified);

        return response.HttpStatusCode == System.Net.HttpStatusCode.OK;
    }


}
```

Créer une fonction qui exécute le scénario.

```
global using System.Threading.Tasks;
global using Amazon.IdentityManagement;
global using Amazon.Lambda;
global using LambdaActions;
global using LambdaScenarioCommon;
global using Microsoft.Extensions.DependencyInjection;
global using Microsoft.Extensions.Hosting;
global using Microsoft.Extensions.Logging;
global using Microsoft.Extensions.Logging.Console;
global using Microsoft.Extensions.Logging.Debug;


using Amazon.Lambda.Model;
using Microsoft.Extensions.Configuration;

namespace LambdaBasics;

public class LambdaBasics
```

```
{
    private static ILogger logger = null!;

    static async Task Main(string[] args)
    {
        // Set up dependency injection for the Amazon service.
        using var host = Host.CreateDefaultBuilder(args)
            .ConfigureLogging(logging =>
                logging.AddFilter("System", LogLevel.Debug)
                    .AddFilter<DebugLoggerProvider>("Microsoft",
 LogLevel.Information)
                    .AddFilter<ConsoleLoggerProvider>("Microsoft",
 LogLevel.Trace))
            .ConfigureServices((_, services) =>
            services.AddAWSService<IAmazonLambda>()
            .AddAWSService<IAmazonIdentityManagementService>()
            .AddTransient<LambdaWrapper>()
            .AddTransient<LambdaRoleWrapper>()
            .AddTransient<UIWrapper>()
        )
        .Build();

        var configuration = new ConfigurationBuilder()
            .SetBasePath(Directory.GetCurrentDirectory())
            .AddJsonFile("settings.json") // Load test settings from .json file.
            .AddJsonFile("settings.local.json",
            true) // Optionally load local settings.
        .Build();


        logger = LoggerFactory.Create(builder => { builder.AddConsole(); })
            .CreateLogger<LambdaBasics>();

        var lambdaWrapper = host.Services.GetRequiredService<LambdaWrapper>();
        var lambdaRoleWrapper =
 host.Services.GetRequiredService<LambdaRoleWrapper>();
        var uiWrapper = host.Services.GetRequiredService<UIWrapper>();

        string functionName = configuration["FunctionName"]!;
        string roleName = configuration["RoleName"]!;
        string policyDocument = "{" +
            " \"Version\": \"2012-10-17\"," +
            " \"Statement\": [ " +
            "    {" +
```

```
            "        \"Effect\": \"Allow\"," +
            "        \"Principal\": {" +
            "            \"Service\": \"lambda.amazonaws.com\" " +
            "    }," +
            "        \"Action\": \"sts:AssumeRole\" " +
            "    }" +
            "]" +
        "}";

        var incrementHandler = configuration["IncrementHandler"];
        var calculatorHandler = configuration["CalculatorHandler"];
        var bucketName = configuration["BucketName"];
        var incrementKey = configuration["IncrementKey"];
        var calculatorKey = configuration["CalculatorKey"];
        var policyArn = configuration["PolicyArn"];

        uiWrapper.DisplayLambdaBasicsOverview();

        // Create the policy to use with the AWS Lambda functions and then attach
the
        // policy to a new role.
        var roleArn = await lambdaRoleWrapper.CreateLambdaRoleAsync(roleName,
policyDocument);

        Console.WriteLine("Waiting for role to become active.");
        uiWrapper.WaitABit(15, "Wait until the role is active before trying to
use it.");

        // Attach the appropriate AWS Identity and Access Management (IAM) role
policy to the new role.
        var success = await
lambdaRoleWrapper.AttachLambdaRolePolicyAsync(policyArn, roleName);
        uiWrapper.WaitABit(10, "Allow time for the IAM policy to be attached to
the role.");

        // Create the Lambda function using a zip file stored in an Amazon Simple
Storage Service
        // (Amazon S3) bucket.
        uiWrapper.DisplayTitle("Create Lambda Function");
        Console.WriteLine($"Creating the AWS Lambda function: {functionName}.");
        var lambdaArn = await lambdaWrapper.CreateLambdaFunctionAsync(
            functionName,
            bucketName,
            incrementKey,
```

```
            roleArn,
            incrementHandler);

        Console.WriteLine("Waiting for the new function to be available.");
        Console.WriteLine($"The AWS Lambda ARN is {lambdaArn}");

        // Get the Lambda function.
        Console.WriteLine($"Getting the {functionName} AWS Lambda function.");
        FunctionConfiguration config;
        do
        {
            config = await lambdaWrapper.GetFunctionAsync(functionName);
            Console.Write(".");
        }
        while (config.State != State.Active);

        Console.WriteLine($"\nThe function, {functionName} has been created.");
        Console.WriteLine($"The runtime of this Lambda function is
{config.Runtime}.");

        uiWrapper.PressEnter();

        // List the Lambda functions.
        uiWrapper.DisplayTitle("Listing all Lambda functions.");
        var functions = await lambdaWrapper.ListFunctionsAsync();
        DisplayFunctionList(functions);

        uiWrapper.DisplayTitle("Invoke increment function");
        Console.WriteLine("Now that it has been created, invoke the Lambda
increment function.");
        string? value;
        do
        {
            Console.Write("Enter a value to increment: ");
            value = Console.ReadLine();
        }
        while (string.IsNullOrEmpty(value));

        string functionParameters = "{" +
            "\"action\": \"increment\", " +
            "\"x\": \"" + value + "\"" +
        "}";
        var answer = await lambdaWrapper.InvokeFunctionAsync(functionName,
functionParameters);
```

```
        Console.WriteLine($"{value} + 1 = {answer}.");

        uiWrapper.DisplayTitle("Update function");
        Console.WriteLine("Now update the Lambda function code.");
        await lambdaWrapper.UpdateFunctionCodeAsync(functionName, bucketName,
calculatorKey);

        do
        {
            config = await lambdaWrapper.GetFunctionAsync(functionName);
            Console.Write(".");
        }
        while (config.LastUpdateStatus == LastUpdateStatus.InProgress);

        await lambdaWrapper.UpdateFunctionConfigurationAsync(
            functionName,
            calculatorHandler,
            new Dictionary<string, string> { { "LOG_LEVEL", "DEBUG" } });

        do
        {
            config = await lambdaWrapper.GetFunctionAsync(functionName);
            Console.Write(".");
        }
        while (config.LastUpdateStatus == LastUpdateStatus.InProgress);

        uiWrapper.DisplayTitle("Call updated function");
        Console.WriteLine("Now call the updated function...");

        bool done = false;

        do
        {
            string? opSelected;

            Console.WriteLine("Select the operation to perform:");
            Console.WriteLine("\t1. add");
            Console.WriteLine("\t2. subtract");
            Console.WriteLine("\t3. multiply");
            Console.WriteLine("\t4. divide");
            Console.WriteLine("\tOr enter \"q\" to quit.");
            Console.WriteLine("Enter the number (1, 2, 3, 4, or q) of the
operation you want to perform: ");
            do
```

```
            {
                Console.Write("Your choice? ");
                opSelected = Console.ReadLine();
            }
            while (opSelected == string.Empty);

            var operation = (opSelected) switch
            {
                "1" => "add",
                "2" => "subtract",
                "3" => "multiply",
                "4" => "divide",
                "q" => "quit",
                _ => "add",
            };

            if (operation == "quit")
            {
                done = true;
            }
            else
            {
                // Get two numbers and an action from the user.
                value = string.Empty;
                do
                {
                    Console.Write("Enter the first value: ");
                    value = Console.ReadLine();
                }
                while (value == string.Empty);

                string? value2;
                do
                {
                    Console.Write("Enter a second value: ");
                    value2 = Console.ReadLine();
                }
                while (value2 == string.Empty);

                functionParameters = "{" +
                    "\"action\": \"" + operation + "\", " +
                    "\"x\": \"" + value + "\"," +
                    "\"y\": \"" + value2 + "\"" +
                "}";
```

```
                answer = await lambdaWrapper.InvokeFunctionAsync(functionName,
functionParameters);
                Console.WriteLine($"The answer when we {operation} the two
numbers is: {answer}.");
            }

            uiWrapper.PressEnter();
        } while (!done);

        // Delete the function created earlier.

        uiWrapper.DisplayTitle("Clean up resources");
        // Detach the IAM policy from the IAM role.
        Console.WriteLine("First detach the IAM policy from the role.");
        success = await lambdaRoleWrapper.DetachLambdaRolePolicyAsync(policyArn,
roleName);
        uiWrapper.WaitABit(15, "Let's wait for the policy to be fully detached
from the role.");

        Console.WriteLine("Delete the AWS Lambda function.");
        success = await lambdaWrapper.DeleteFunctionAsync(functionName);
        if (success)
        {
            Console.WriteLine($"The {functionName} function was deleted.");
        }
        else
        {
            Console.WriteLine($"Could not remove the function {functionName}");
        }

        // Now delete the IAM role created for use with the functions
        // created by the application.
        Console.WriteLine("Now we can delete the role that we created.");
        success = await lambdaRoleWrapper.DeleteLambdaRoleAsync(roleName);
        if (success)
        {
            Console.WriteLine("The role has been successfully removed.");
        }
        else
        {
            Console.WriteLine("Couldn't delete the role.");
        }
```

```
        Console.WriteLine("The Lambda Scenario is now complete.");
        uiWrapper.PressEnter();

        // Displays a formatted list of existing functions returned by the
        // LambdaMethods.ListFunctions.
        void DisplayFunctionList(List<FunctionConfiguration> functions)
        {
            functions.ForEach(functionConfig =>
            {

 Console.WriteLine($"{functionConfig.FunctionName}\t{functionConfig.Description}");
            });
        }
    }
}


namespace LambdaActions;

using Amazon.IdentityManagement;
using Amazon.IdentityManagement.Model;

public class LambdaRoleWrapper
{
    private readonly IAmazonIdentityManagementService _lambdaRoleService;

    public LambdaRoleWrapper(IAmazonIdentityManagementService lambdaRoleService)
    {
        _lambdaRoleService = lambdaRoleService;
    }

    /// <summary>
    /// Attach an AWS Identity and Access Management (IAM) role policy to the
    /// IAM role to be assumed by the AWS Lambda functions created for the
 scenario.
    /// </summary>
    /// <param name="policyArn">The Amazon Resource Name (ARN) of the IAM
 policy.</param>
    /// <param name="roleName">The name of the IAM role to attach the IAM policy
 to.</param>
    /// <returns>A Boolean value indicating the success of the action.</returns>
    public async Task<bool> AttachLambdaRolePolicyAsync(string policyArn, string
 roleName)
    {
```

```
        var response = await _lambdaRoleService.AttachRolePolicyAsync(new
 AttachRolePolicyRequest { PolicyArn = policyArn, RoleName = roleName });
        return response.HttpStatusCode == System.Net.HttpStatusCode.OK;
    }

    /// <summary>
    /// Create a new IAM role.
    /// </summary>
    /// <param name="roleName">The name of the IAM role to create.</param>
    /// <param name="policyDocument">The policy document for the new IAM role.</
param>
    /// <returns>A string representing the ARN for newly created role.</returns>
    public async Task<string> CreateLambdaRoleAsync(string roleName, string
 policyDocument)
    {
        var request = new CreateRoleRequest
        {
            AssumeRolePolicyDocument = policyDocument,
            RoleName = roleName,
        };

        var response = await _lambdaRoleService.CreateRoleAsync(request);
        return response.Role.Arn;
    }

    /// <summary>
    /// Deletes an IAM role.
    /// </summary>
    /// <param name="roleName">The name of the role to delete.</param>
    /// <returns>A Boolean value indicating the success of the operation.</
returns>
    public async Task<bool> DeleteLambdaRoleAsync(string roleName)
    {
        var request = new DeleteRoleRequest
        {
            RoleName = roleName,
        };

        var response = await _lambdaRoleService.DeleteRoleAsync(request);
        return response.HttpStatusCode == System.Net.HttpStatusCode.OK;
    }

    public async Task<bool> DetachLambdaRolePolicyAsync(string policyArn, string
 roleName)
```

```
    {
        var response = await _lambdaRoleService.DetachRolePolicyAsync(new
 DetachRolePolicyRequest { PolicyArn = policyArn, RoleName = roleName });
        return response.HttpStatusCode == System.Net.HttpStatusCode.OK;
    }
}


namespace LambdaScenarioCommon;

public class UIWrapper
{
    public readonly string SepBar = new('-', Console.WindowWidth);

    /// <summary>
    /// Show information about the AWS Lambda Basics scenario.
    /// </summary>
    public void DisplayLambdaBasicsOverview()
    {
        Console.Clear();

        DisplayTitle("Welcome to AWS Lambda Basics");
        Console.WriteLine("This example application does the following:");
        Console.WriteLine("\t1. Creates an AWS Identity and Access Management
 (IAM) role that will be assumed by the functions we create.");
        Console.WriteLine("\t2. Attaches an IAM role policy that has Lambda
 permissions.");
        Console.WriteLine("\t3. Creates a Lambda function that increments the
 value passed to it.");
        Console.WriteLine("\t4. Calls the increment function and passes a
 value.");
        Console.WriteLine("\t5. Updates the code so that the function is a simple
 calculator.");
        Console.WriteLine("\t6. Calls the calculator function with the values
 entered.");
        Console.WriteLine("\t7. Deletes the Lambda function.");
        Console.WriteLine("\t7. Detaches the IAM role policy.");
        Console.WriteLine("\t8. Deletes the IAM role.");
        PressEnter();
    }

    /// <summary>
    /// Display a message and wait until the user presses enter.
    /// </summary>
```

```
    public void PressEnter()
    {
        Console.Write("\nPress <Enter> to continue. ");
        _ = Console.ReadLine();
        Console.WriteLine();
    }

    /// <summary>
    /// Pad a string with spaces to center it on the console display.
    /// </summary>
    /// <param name="strToCenter">The string to be centered.</param>
    /// <returns>The padded string.</returns>
    public string CenterString(string strToCenter)
    {
        var padAmount = (Console.WindowWidth - strToCenter.Length) / 2;
        var leftPad = new string(' ', padAmount);
        return $"{leftPad}{strToCenter}";
    }

    /// <summary>
    /// Display a line of hyphens, the centered text of the title and another
    /// line of hyphens.
    /// </summary>
    /// <param name="strTitle">The string to be displayed.</param>
    public void DisplayTitle(string strTitle)
    {
        Console.WriteLine(SepBar);
        Console.WriteLine(CenterString(strTitle));
        Console.WriteLine(SepBar);
    }

    /// <summary>
    /// Display a countdown and wait for a number of seconds.
    /// </summary>
    /// <param name="numSeconds">The number of seconds to wait.</param>
    public void WaitABit(int numSeconds, string msg)
    {
        Console.WriteLine(msg);

        // Wait for the requested number of seconds.
        for (int i = numSeconds; i > 0; i--)
        {
            System.Threading.Thread.Sleep(1000);
            Console.Write($"{i}...");
```

```
        }

        PressEnter();
    }
}
```

Définir un gestionnaire Lambda qui incrémente un nombre.

```
using Amazon.Lambda.Core;

// Assembly attribute to enable the Lambda function's JSON input to be converted
 into a .NET class.
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSeri

namespace LambdaIncrement;

public class Function
{

    /// <summary>
    /// A simple function increments the integer parameter.
    /// </summary>
    /// <param name="input">A JSON string containing an action, which must be
    /// "increment" and a string representing the value to increment.</param>
    /// <param name="context">The context object passed by Lambda containing
    /// information about invocation, function, and execution environment.</
param>
    /// <returns>A string representing the incremented value of the parameter.</
returns>
    public int FunctionHandler(Dictionary<string, string> input, ILambdaContext
 context)
    {
        if (input["action"] == "increment")
        {
            int inputValue = Convert.ToInt32(input["x"]);
            return inputValue + 1;
        }
        else
        {
            return 0;
```

```
        }
    }
}
```

Définir un deuxième gestionnaire Lambda qui effectue des opérations arithmétiques.

```
using Amazon.Lambda.Core;

// Assembly attribute to enable the Lambda function's JSON input to be converted
 into a .NET class.
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSeri

namespace LambdaCalculator;

public class Function
{

    /// <summary>
    /// A simple function that takes two number in string format and performs
    /// the requested arithmetic function.
    /// </summary>
    /// <param name="input">JSON data containing an action, and x and y values.
    /// Valid actions include: add, subtract, multiply, and divide.</param>
    /// <param name="context">The context object passed by Lambda containing
    /// information about invocation, function, and execution environment.</
param>
    /// <returns>A string representing the results of the calculation.</returns>
    public int FunctionHandler(Dictionary<string, string> input, ILambdaContext
 context)
    {
        var action = input["action"];
        int x = Convert.ToInt32(input["x"]);
        int y = Convert.ToInt32(input["y"]);
        int result;
        switch (action)
        {
            case "add":
                result = x + y;
                break;
            case "subtract":
```

```
                result = x - y;
                break;
            case "multiply":
                result = x * y;
                break;
            case "divide":
                if (y == 0)
                {
                    Console.Error.WriteLine("Divide by zero error.");
                    result = 0;
                }
                else
                    result = x / y;
                break;
            default:
                Console.Error.WriteLine($"{action} is not a valid operation.");
                result = 0;
                break;
        }
        return result;
    }
}
```

- Pour plus d'informations sur l'API, consultez les rubriques suivantes dans la référence de l'API AWS SDK pour .NET .
  - CreateFunction
  - DeleteFunction
  - GetFunction
  - Invoke
  - ListFunctions
  - UpdateFunctionCode
  - UpdateFunctionConfiguration

C++

SDK pour C++

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
//! Get started with functions scenario.
/*!
 \param clientConfig: AWS client configuration.
 \return bool: Successful completion.
 */
bool AwsDoc::Lambda::getStartedWithFunctionsScenario(
        const Aws::Client::ClientConfiguration &clientConfig) {

    Aws::Lambda::LambdaClient client(clientConfig);

    // 1. Create an AWS Identity and Access Management (IAM) role for Lambda
 function.
    Aws::String roleArn;
    if (!getIamRoleArn(roleArn, clientConfig)) {
        return false;
    }

    // 2. Create a Lambda function.
    int seconds = 0;
    do {
        Aws::Lambda::Model::CreateFunctionRequest request;
        request.SetFunctionName(LAMBDA_NAME);
        request.SetDescription(LAMBDA_DESCRIPTION); // Optional.
#if USE_CPP_LAMBDA_FUNCTION
        request.SetRuntime(Aws::Lambda::Model::Runtime::provided_al2);
        request.SetTimeout(15);
        request.SetMemorySize(128);

        // Assume the AWS Lambda function was built in Docker with same
 architecture
        // as this code.
#if  defined(__x86_64__)
```

```
        request.SetArchitectures({Aws::Lambda::Model::Architecture::x86_64});
#elif defined(__aarch64__)
        request.SetArchitectures({Aws::Lambda::Model::Architecture::arm64});
#else
#error "Unimplemented architecture"
#endif // defined(architecture)
#else
        request.SetRuntime(Aws::Lambda::Model::Runtime::python3_9);
#endif
        request.SetRole(roleArn);
        request.SetHandler(LAMBDA_HANDLER_NAME);
        request.SetPublish(true);
        Aws::Lambda::Model::FunctionCode code;
        std::ifstream ifstream(INCREMENT_LAMBDA_CODE.c_str(),
                               std::ios_base::in | std::ios_base::binary);
        if (!ifstream.is_open()) {
            std::cerr << "Error opening file " << INCREMENT_LAMBDA_CODE << "." <<
 std::endl;

#if USE_CPP_LAMBDA_FUNCTION
            std::cerr
                    << "The cpp Lambda function must be built following the
 instructions in the cpp_lambda/README.md file. "
                    << std::endl;
#endif
            deleteIamRole(clientConfig);
            return false;
        }

        Aws::StringStream buffer;
        buffer << ifstream.rdbuf();

        code.SetZipFile(Aws::Utils::ByteBuffer((unsigned char *)
 buffer.str().c_str(),
                                               buffer.str().length()));
        request.SetCode(code);

        Aws::Lambda::Model::CreateFunctionOutcome outcome =
 client.CreateFunction(
                request);

        if (outcome.IsSuccess()) {
            std::cout << "The lambda function was successfully created. " <<
 seconds
```

```
                    << " seconds elapsed." << std::endl;
            break;
        }
        else if (outcome.GetError().GetErrorType() ==
                 Aws::Lambda::LambdaErrors::INVALID_PARAMETER_VALUE &&
                 outcome.GetError().GetMessage().find("role") >= 0) {
            if ((seconds % 5) == 0) { // Log status every 10 seconds.
                std::cout
                        << "Waiting for the IAM role to become available as a
CreateFunction parameter. "
                        << seconds
                        << " seconds elapsed." << std::endl;

                std::cout << outcome.GetError().GetMessage() << std::endl;
            }
        }
        else {
            std::cerr << "Error with CreateFunction. "
                      << outcome.GetError().GetMessage()
                      << std::endl;
            deleteIamRole(clientConfig);
            return false;
        }
        ++seconds;
        std::this_thread::sleep_for(std::chrono::seconds(1));
    } while (60 > seconds);

    std::cout << "The current Lambda function increments 1 by an input." <<
std::endl;

    // 3.  Invoke the Lambda function.
    {
        int increment = askQuestionForInt("Enter an increment integer: ");

        Aws::Lambda::Model::InvokeResult invokeResult;
        Aws::Utils::Json::JsonValue jsonPayload;
        jsonPayload.WithString("action", "increment");
        jsonPayload.WithInteger("number", increment);
        if (invokeLambdaFunction(jsonPayload, Aws::Lambda::Model::LogType::Tail,
                                 invokeResult, client)) {
            Aws::Utils::Json::JsonValue jsonValue(invokeResult.GetPayload());
            Aws::Map<Aws::String, Aws::Utils::Json::JsonView> values =
                    jsonValue.View().GetAllObjects();
            auto iter = values.find("result");
```

```
            if (iter != values.end() && iter->second.IsIntegerType()) {
                {
                    std::cout << INCREMENT_RESUlT_PREFIX
                              << iter->second.AsInteger() << std::endl;
                }
            }
            else {
                std::cout << "There was an error in execution. Here is the log."
                          << std::endl;
                Aws::Utils::ByteBuffer buffer =
 Aws::Utils::HashingUtils::Base64Decode(
                        invokeResult.GetLogResult());
                std::cout << "With log " << buffer.GetUnderlyingData() <<
 std::endl;
            }
        }
    }

    std::cout
            << "The Lambda function will now be updated with new code. Press
 return to continue, ";
    Aws::String answer;
    std::getline(std::cin, answer);

    // 4.  Update the Lambda function code.
    {
        Aws::Lambda::Model::UpdateFunctionCodeRequest request;
        request.SetFunctionName(LAMBDA_NAME);
        std::ifstream ifstream(CALCULATOR_LAMBDA_CODE.c_str(),
                               std::ios_base::in | std::ios_base::binary);
        if (!ifstream.is_open()) {
            std::cerr << "Error opening file " << INCREMENT_LAMBDA_CODE << "." <<
 std::endl;

#if USE_CPP_LAMBDA_FUNCTION
            std::cerr
                    << "The cpp Lambda function must be built following the
 instructions in the cpp_lambda/README.md file. "
                    << std::endl;
#endif
            deleteLambdaFunction(client);
            deleteIamRole(clientConfig);
            return false;
        }
```

```
        Aws::StringStream buffer;
        buffer << ifstream.rdbuf();
        request.SetZipFile(
                Aws::Utils::ByteBuffer((unsigned char *) buffer.str().c_str(),
                                       buffer.str().length()));
        request.SetPublish(true);

        Aws::Lambda::Model::UpdateFunctionCodeOutcome outcome =
client.UpdateFunctionCode(
                request);

        if (outcome.IsSuccess()) {
            std::cout << "The lambda code was successfully updated." <<
std::endl;
        }
        else {
            std::cerr << "Error with Lambda::UpdateFunctionCode. "
                      << outcome.GetError().GetMessage()
                      << std::endl;
        }
    }

    std::cout
              << "This function uses an environment variable to control the logging
level."
              << std::endl;
    std::cout
              << "UpdateFunctionConfiguration will be used to set the LOG_LEVEL to
DEBUG."
              << std::endl;
    seconds = 0;

    // 5.  Update the Lambda function configuration.
    do {
        ++seconds;
        std::this_thread::sleep_for(std::chrono::seconds(1));
        Aws::Lambda::Model::UpdateFunctionConfigurationRequest request;
        request.SetFunctionName(LAMBDA_NAME);
        Aws::Lambda::Model::Environment environment;
        environment.AddVariables("LOG_LEVEL", "DEBUG");
        request.SetEnvironment(environment);
```

```
        Aws::Lambda::Model::UpdateFunctionConfigurationOutcome outcome =
 client.UpdateFunctionConfiguration(
                request);

        if (outcome.IsSuccess()) {
            std::cout << "The lambda configuration was successfully updated."
                      << std::endl;
            break;
        }

            // RESOURCE_IN_USE: function code update not completed.
        else if (outcome.GetError().GetErrorType() !=
                 Aws::Lambda::LambdaErrors::RESOURCE_IN_USE) {
            if ((seconds % 10) == 0) { // Log status every 10 seconds.
                std::cout << "Lambda function update in progress . After " <<
 seconds
                          << " seconds elapsed." << std::endl;
            }
        }
        else {
            std::cerr << "Error with Lambda::UpdateFunctionConfiguration. "
                      << outcome.GetError().GetMessage()
                      << std::endl;
        }

    } while (0 < seconds);

    if (0 > seconds) {
        std::cerr << "Function failed to become active." << std::endl;
    }
    else {
        std::cout << "Updated function active after " << seconds << " seconds."
                  << std::endl;
    }

    std::cout
            << "\nThe new code applies an arithmetic operator to two variables, x
 an y."
            << std::endl;
    std::vector<Aws::String> operators = {"plus", "minus", "times", "divided-
by"};
    for (size_t i = 0; i < operators.size(); ++i) {
        std::cout << "   " << i + 1 << " " << operators[i] << std::endl;
    }
```

```
   // 6.  Invoke the updated Lambda function.
   do {
       int operatorIndex = askQuestionForIntRange("Select an operator index 1 -
4 ", 1,
                                                  4);
       int x = askQuestionForInt("Enter an integer for the x value ");
       int y = askQuestionForInt("Enter an integer for the y value ");

       Aws::Utils::Json::JsonValue calculateJsonPayload;
       calculateJsonPayload.WithString("action", operators[operatorIndex - 1]);
       calculateJsonPayload.WithInteger("x", x);
       calculateJsonPayload.WithInteger("y", y);
       Aws::Lambda::Model::InvokeResult calculatedResult;
       if (invokeLambdaFunction(calculateJsonPayload,
                                Aws::Lambda::Model::LogType::Tail,
                                calculatedResult, client)) {
           Aws::Utils::Json::JsonValue jsonValue(calculatedResult.GetPayload());
           Aws::Map<Aws::String, Aws::Utils::Json::JsonView> values =
                   jsonValue.View().GetAllObjects();
           auto iter = values.find("result");
           if (iter != values.end() && iter->second.IsIntegerType()) {
               std::cout << ARITHMETIC_RESULT_PREFIX << x << " "
                         << operators[operatorIndex - 1] << " "
                         << y << " is " << iter->second.AsInteger() <<
std::endl;
           }
           else if (iter != values.end() && iter->second.IsFloatingPointType())
{
               std::cout << ARITHMETIC_RESULT_PREFIX << x << " "
                         << operators[operatorIndex - 1] << " "
                         << y << " is " << iter->second.AsDouble() << std::endl;
           }
           else {
               std::cout << "There was an error in execution. Here is the log."
                         << std::endl;
               Aws::Utils::ByteBuffer buffer =
Aws::Utils::HashingUtils::Base64Decode(
                        calculatedResult.GetLogResult());
               std::cout << "With log " << buffer.GetUnderlyingData() <<
std::endl;
           }
       }
```

```
        answer = askQuestion("Would you like to try another operation? (y/n) ");
    } while (answer == "y");

    std::cout
            << "A list of the lambda functions will be retrieved. Press return to
continue, ";
    std::getline(std::cin, answer);

    // 7.  List the Lambda functions.

    std::vector<Aws::String> functions;
    Aws::String marker;

    do {
        Aws::Lambda::Model::ListFunctionsRequest request;
        if (!marker.empty()) {
            request.SetMarker(marker);
        }

        Aws::Lambda::Model::ListFunctionsOutcome outcome = client.ListFunctions(
                request);

        if (outcome.IsSuccess()) {
            const Aws::Lambda::Model::ListFunctionsResult &result =
outcome.GetResult();
            std::cout << result.GetFunctions().size()
                      << " lambda functions were retrieved." << std::endl;

            for (const Aws::Lambda::Model::FunctionConfiguration
&functionConfiguration: result.GetFunctions()) {
                functions.push_back(functionConfiguration.GetFunctionName());
                std::cout << functions.size() << "  "
                          << functionConfiguration.GetDescription() << std::endl;
                std::cout << "   "
                          <<
Aws::Lambda::Model::RuntimeMapper::GetNameForRuntime(
                                  functionConfiguration.GetRuntime()) << ": "
                          << functionConfiguration.GetHandler()
                          << std::endl;
            }
            marker = result.GetNextMarker();
        }
        else {
            std::cerr << "Error with Lambda::ListFunctions. "
```

```
                    << outcome.GetError().GetMessage()
                    << std::endl;
        }
    } while (!marker.empty());

    // 8.  Get a Lambda function.
    if (!functions.empty()) {
        std::stringstream question;
        question << "Choose a function to retrieve between 1 and " <<
functions.size()
                 << " ";
        int functionIndex = askQuestionForIntRange(question.str(), 1,

static_cast<int>(functions.size()));

        Aws::String functionName = functions[functionIndex - 1];

        Aws::Lambda::Model::GetFunctionRequest request;
        request.SetFunctionName(functionName);

        Aws::Lambda::Model::GetFunctionOutcome outcome =
client.GetFunction(request);

        if (outcome.IsSuccess()) {
            std::cout << "Function retrieve.\n" <<

outcome.GetResult().GetConfiguration().Jsonize().View().WriteReadable()
                    << std::endl;
        }
        else {
            std::cerr << "Error with Lambda::GetFunction. "
                    << outcome.GetError().GetMessage()
                    << std::endl;
        }
    }

    std::cout << "The resources will be deleted. Press return to continue, ";
    std::getline(std::cin, answer);

    // 9.  Delete the Lambda function.
    bool result = deleteLambdaFunction(client);

    // 10. Delete the IAM role.
    return result && deleteIamRole(clientConfig);
```

```
}

//! Routine which invokes a Lambda function and returns the result.
/*!
 \param jsonPayload: Payload for invoke function.
 \param logType: Log type setting for invoke function.
 \param invokeResult: InvokeResult object to receive the result.
 \param client: Lambda client.
 \return bool: Successful completion.
 */
bool
AwsDoc::Lambda::invokeLambdaFunction(const Aws::Utils::Json::JsonValue
 &jsonPayload,
                                     Aws::Lambda::Model::LogType logType,
                                     Aws::Lambda::Model::InvokeResult
 &invokeResult,
                                     const Aws::Lambda::LambdaClient &client) {
    int seconds = 0;
    bool result = false;
    /*
     * In this example, the Invoke function can be called before recently created
 resources are
     * available.  The Invoke function is called repeatedly until the resources
 are
     * available.
     */
    do {
        Aws::Lambda::Model::InvokeRequest request;
        request.SetFunctionName(LAMBDA_NAME);
        request.SetLogType(logType);
        std::shared_ptr<Aws::IOStream> payload =
 Aws::MakeShared<Aws::StringStream>(
                "FunctionTest");
        *payload << jsonPayload.View().WriteReadable();
        request.SetBody(payload);
        request.SetContentType("application/json");
        Aws::Lambda::Model::InvokeOutcome outcome = client.Invoke(request);

        if (outcome.IsSuccess()) {
            invokeResult = std::move(outcome.GetResult());
            result = true;
            break;
        }
```

```
            // ACCESS_DENIED: because the role is not available yet.
            // RESOURCE_CONFLICT: because the Lambda function is being created or
 updated.
        else if ((outcome.GetError().GetErrorType() ==
                  Aws::Lambda::LambdaErrors::ACCESS_DENIED) ||
                 (outcome.GetError().GetErrorType() ==
                  Aws::Lambda::LambdaErrors::RESOURCE_CONFLICT)) {
            if ((seconds % 5) == 0) { // Log status every 10 seconds.
                std::cout << "Waiting for the invoke api to be available, status
 " <<
                          ((outcome.GetError().GetErrorType() ==
                            Aws::Lambda::LambdaErrors::ACCESS_DENIED ?
                            "ACCESS_DENIED" : "RESOURCE_CONFLICT")) << ". " <<
 seconds
                          << " seconds elapsed." << std::endl;
            }
        }
        else {
            std::cerr << "Error with Lambda::InvokeRequest. "
                      << outcome.GetError().GetMessage()
                      << std::endl;
            break;
        }
        ++seconds;
        std::this_thread::sleep_for(std::chrono::seconds(1));
    } while (seconds < 60);

    return result;
}
```

- Pour plus de détails sur l'API, consultez les rubriques suivantes dans la Référence des API du kit AWS SDK pour C++ .
  - CreateFunction
  - DeleteFunction
  - GetFunction
  - Invoke
  - ListFunctions
  - UpdateFunctionCode
  - UpdateFunctionConfiguration

Go

Kit SDK pour Go V2

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Créez un scénario interactif qui vous montre comment démarrer avec les fonctions Lambda.

```
import (
 "archive/zip"
 "bytes"
 "context"
 "encoding/base64"
 "encoding/json"
 "errors"
 "fmt"
 "log"
 "os"
 "strings"
 "time"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/service/iam"
 iamtypes "github.com/aws/aws-sdk-go-v2/service/iam/types"
 "github.com/aws/aws-sdk-go-v2/service/lambda"
 "github.com/awsdocs/aws-doc-sdk-examples/gov2/demotools"
 "github.com/awsdocs/aws-doc-sdk-examples/gov2/lambda/actions"
)

// GetStartedFunctionsScenario shows you how to use AWS Lambda to perform the
 following
// actions:
//
//  1. Create an AWS Identity and Access Management (IAM) role and Lambda
 function, then upload handler code.
//  2. Invoke the function with a single parameter and get results.
//  3. Update the function code and configure with an environment variable.
```

```
//  4. Invoke the function with new parameters and get results. Display the
 returned execution log.
//  5. List the functions for your account, then clean up resources.
type GetStartedFunctionsScenario struct {
 sdkConfig       aws.Config
 functionWrapper actions.FunctionWrapper
 questioner      demotools.IQuestioner
 helper          IScenarioHelper
 isTestRun       bool
}

// NewGetStartedFunctionsScenario constructs a GetStartedFunctionsScenario
 instance from a configuration.
// It uses the specified config to get a Lambda client and create wrappers for
 the actions
// used in the scenario.
func NewGetStartedFunctionsScenario(sdkConfig aws.Config, questioner
 demotools.IQuestioner,
 helper IScenarioHelper) GetStartedFunctionsScenario {
 lambdaClient := lambda.NewFromConfig(sdkConfig)
 return GetStartedFunctionsScenario{
  sdkConfig:       sdkConfig,
  functionWrapper: actions.FunctionWrapper{LambdaClient: lambdaClient},
  questioner:      questioner,
  helper:          helper,
 }
}

// Run runs the interactive scenario.
func (scenario GetStartedFunctionsScenario) Run(ctx context.Context) {
 defer func() {
  if r := recover(); r != nil {
   log.Printf("Something went wrong with the demo.\n")
  }
 }()

 log.Println(strings.Repeat("-", 88))
 log.Println("Welcome to the AWS Lambda get started with functions demo.")
 log.Println(strings.Repeat("-", 88))

 role := scenario.GetOrCreateRole(ctx)
 funcName := scenario.CreateFunction(ctx, role)
 scenario.InvokeIncrement(ctx, funcName)
 scenario.UpdateFunction(ctx, funcName)
```

```
 scenario.InvokeCalculator(ctx, funcName)
 scenario.ListFunctions(ctx)
 scenario.Cleanup(ctx, role, funcName)

 log.Println(strings.Repeat("-", 88))
 log.Println("Thanks for watching!")
 log.Println(strings.Repeat("-", 88))
}

// GetOrCreateRole checks whether the specified role exists and returns it if it
 does.
// Otherwise, a role is created that specifies Lambda as a trusted principal.
// The AWSLambdaBasicExecutionRole managed policy is attached to the role and the
 role
// is returned.
func (scenario GetStartedFunctionsScenario) GetOrCreateRole(ctx context.Context)
 *iamtypes.Role {
 var role *iamtypes.Role
 iamClient := iam.NewFromConfig(scenario.sdkConfig)
 log.Println("First, we need an IAM role that Lambda can assume.")
 roleName := scenario.questioner.Ask("Enter a name for the role:",
 demotools.NotEmpty{})
 getOutput, err := iamClient.GetRole(ctx, &iam.GetRoleInput{
  RoleName: aws.String(roleName)})
 if err != nil {
  var noSuch *iamtypes.NoSuchEntityException
  if errors.As(err, &noSuch) {
   log.Printf("Role %v doesn't exist. Creating it....\n", roleName)
  } else {
   log.Panicf("Couldn't check whether role %v exists. Here's why: %v\n",
    roleName, err)
  }
 } else {
  role = getOutput.Role
  log.Printf("Found role %v.\n", *role.RoleName)
 }
 if role == nil {
  trustPolicy := PolicyDocument{
   Version: "2012-10-17",
   Statement: []PolicyStatement{{
    Effect:    "Allow",
    Principal: map[string]string{"Service": "lambda.amazonaws.com"},
    Action:    []string{"sts:AssumeRole"},
   }},
```

```
  }
  policyArn := "arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole"
  createOutput, err := iamClient.CreateRole(ctx, &iam.CreateRoleInput{
   AssumeRolePolicyDocument: aws.String(trustPolicy.String()),
   RoleName:                 aws.String(roleName),
  })
  if err != nil {
   log.Panicf("Couldn't create role %v. Here's why: %v\n", roleName, err)
  }
  role = createOutput.Role
  _, err = iamClient.AttachRolePolicy(ctx, &iam.AttachRolePolicyInput{
   PolicyArn: aws.String(policyArn),
   RoleName:  aws.String(roleName),
  })
  if err != nil {
   log.Panicf("Couldn't attach a policy to role %v. Here's why: %v\n", roleName,
 err)
  }
  log.Printf("Created role %v.\n", *role.RoleName)
  log.Println("Let's give AWS a few seconds to propagate resources...")
  scenario.helper.Pause(10)
 }
 log.Println(strings.Repeat("-", 88))
 return role
}

// CreateFunction creates a Lambda function and uploads a handler written in
 Python.
// The code for the Python handler is packaged as a []byte in .zip format.
func (scenario GetStartedFunctionsScenario) CreateFunction(ctx context.Context,
 role *iamtypes.Role) string {
 log.Println("Let's create a function that increments a number.\n" +
  "The function uses the 'lambda_handler_basic.py' script found in the \n" +
  "'handlers' directory of this project.")
 funcName := scenario.questioner.Ask("Enter a name for the Lambda function:",
 demotools.NotEmpty{})
 zipPackage := scenario.helper.CreateDeploymentPackage("lambda_handler_basic.py",
 fmt.Sprintf("%v.py", funcName))
 log.Printf("Creating function %v and waiting for it to be ready.", funcName)
 funcState := scenario.functionWrapper.CreateFunction(ctx, funcName,
 fmt.Sprintf("%v.lambda_handler", funcName),
  role.Arn, zipPackage)
 log.Printf("Your function is %v.", funcState)
 log.Println(strings.Repeat("-", 88))
```

```
 return funcName
}

// InvokeIncrement invokes a Lambda function that increments a number. The
 function
// parameters are contained in a Go struct that is used to serialize the
 parameters to
// a JSON payload that is passed to the function.
// The result payload is deserialized into a Go struct that contains an int
 value.
func (scenario GetStartedFunctionsScenario) InvokeIncrement(ctx context.Context,
 funcName string) {
 parameters := actions.IncrementParameters{Action: "increment"}
 log.Println("Let's invoke our function. This function increments a number.")
 parameters.Number = scenario.questioner.AskInt("Enter a number to increment:",
 demotools.NotEmpty{})
 log.Printf("Invoking %v with %v...\n", funcName, parameters.Number)
 invokeOutput := scenario.functionWrapper.Invoke(ctx, funcName, parameters,
 false)
 var payload actions.LambdaResultInt
 err := json.Unmarshal(invokeOutput.Payload, &payload)
 if err != nil {
  log.Panicf("Couldn't unmarshal payload from invoking %v. Here's why: %v\n",
   funcName, err)
 }
 log.Printf("Invoking %v with %v returned %v.\n", funcName, parameters.Number,
 payload)
 log.Println(strings.Repeat("-", 88))
}

// UpdateFunction updates the code for a Lambda function by uploading a simple
 arithmetic
// calculator written in Python. The code for the Python handler is packaged as a
// []byte in .zip format.
// After the code is updated, the configuration is also updated with a new log
// level that instructs the handler to log additional information.
func (scenario GetStartedFunctionsScenario) UpdateFunction(ctx context.Context,
 funcName string) {
 log.Println("Let's update the function to an arithmetic calculator.\n" +
  "The function uses the 'lambda_handler_calculator.py' script found in the \n" +
  "'handlers' directory of this project.")
 scenario.questioner.Ask("Press Enter when you're ready.")
 log.Println("Creating deployment package...")
```

```
 zipPackage :=
 scenario.helper.CreateDeploymentPackage("lambda_handler_calculator.py",
  fmt.Sprintf("%v.py", funcName))
 log.Println("...and updating the Lambda function and waiting for it to be
 ready.")
 funcState := scenario.functionWrapper.UpdateFunctionCode(ctx, funcName,
 zipPackage)
 log.Printf("Updated function %v. Its current state is %v.", funcName, funcState)
 log.Println("This function uses an environment variable to control logging
 level.")
 log.Println("Let's set it to DEBUG to get the most logging.")
 scenario.functionWrapper.UpdateFunctionConfiguration(ctx, funcName,
  map[string]string{"LOG_LEVEL": "DEBUG"})
 log.Println(strings.Repeat("-", 88))
}

// InvokeCalculator invokes the Lambda calculator function. The parameters are
 stored in a
// Go struct that is used to serialize the parameters to a JSON payload. That
 payload is then passed
// to the function.
// The result payload is deserialized to a Go struct that stores the result as
 either an
// int or float32, depending on the kind of operation that was specified.
func (scenario GetStartedFunctionsScenario) InvokeCalculator(ctx context.Context,
 funcName string) {
 wantInvoke := true
 choices := []string{"plus", "minus", "times", "divided-by"}
 for wantInvoke {
  choice := scenario.questioner.AskChoice("Select an arithmetic operation:\n",
 choices)
  x := scenario.questioner.AskInt("Enter a value for x:", demotools.NotEmpty{})
  y := scenario.questioner.AskInt("Enter a value for y:", demotools.NotEmpty{})
  log.Printf("Invoking %v %v %v...", x, choices[choice], y)
  calcParameters := actions.CalculatorParameters{
   Action: choices[choice],
   X:      x,
   Y:      y,
  }
  invokeOutput := scenario.functionWrapper.Invoke(ctx, funcName, calcParameters,
 true)
  var payload any
  if choice == 3 { // divide-by results in a float.
   payload = actions.LambdaResultFloat{}
```

```
  } else {
   payload = actions.LambdaResultInt{}
  }
  err := json.Unmarshal(invokeOutput.Payload, &payload)
  if err != nil {
   log.Panicf("Couldn't unmarshal payload from invoking %v. Here's why: %v\n",
    funcName, err)
  }
  log.Printf("Invoking %v with %v %v %v returned %v.\n", funcName,
   calcParameters.X, calcParameters.Action, calcParameters.Y, payload)
  scenario.questioner.Ask("Press Enter to see the logs from the call.")
  logRes, err := base64.StdEncoding.DecodeString(*invokeOutput.LogResult)
  if err != nil {
   log.Panicf("Couldn't decode log result. Here's why: %v\n", err)
  }
  log.Println(string(logRes))
  wantInvoke = scenario.questioner.AskBool("Do you want to calculate again? (y/
n)", "y")
 }
 log.Println(strings.Repeat("-", 88))
}

// ListFunctions lists up to the specified number of functions for your account.
func (scenario GetStartedFunctionsScenario) ListFunctions(ctx context.Context) {
 count := scenario.questioner.AskInt(
  "Let's list functions for your account. How many do you want to see?",
 demotools.NotEmpty{})
 functions := scenario.functionWrapper.ListFunctions(ctx, count)
 log.Printf("Found %v functions:", len(functions))
 for _, function := range functions {
  log.Printf("\t%v", *function.FunctionName)
 }
 log.Println(strings.Repeat("-", 88))
}

// Cleanup removes the IAM and Lambda resources created by the example.
func (scenario GetStartedFunctionsScenario) Cleanup(ctx context.Context, role
 *iamtypes.Role, funcName string) {
 if scenario.questioner.AskBool("Do you want to clean up resources created for
 this example? (y/n)",
  "y") {
  iamClient := iam.NewFromConfig(scenario.sdkConfig)
  policiesOutput, err := iamClient.ListAttachedRolePolicies(ctx,
   &iam.ListAttachedRolePoliciesInput{RoleName: role.RoleName})
```

```
  if err != nil {
   log.Panicf("Couldn't get policies attached to role %v. Here's why: %v\n",
    *role.RoleName, err)
  }
  for _, policy := range policiesOutput.AttachedPolicies {
   _, err = iamClient.DetachRolePolicy(ctx, &iam.DetachRolePolicyInput{
    PolicyArn: policy.PolicyArn, RoleName: role.RoleName,
   })
   if err != nil {
    log.Panicf("Couldn't detach policy %v from role %v. Here's why: %v\n",
     *policy.PolicyArn, *role.RoleName, err)
   }
  }
  _, err = iamClient.DeleteRole(ctx, &iam.DeleteRoleInput{RoleName:
 role.RoleName})
  if err != nil {
   log.Panicf("Couldn't delete role %v. Here's why: %v\n", *role.RoleName, err)
  }
  log.Printf("Deleted role %v.\n", *role.RoleName)

  scenario.functionWrapper.DeleteFunction(ctx, funcName)
  log.Printf("Deleted function %v.\n", funcName)
 } else {
  log.Println("Okay. Don't forget to delete the resources when you're done with
 them.")
 }
}

// IScenarioHelper abstracts I/O and wait functions from a scenario so that they
// can be mocked for unit testing.
type IScenarioHelper interface {
 Pause(secs int)
 CreateDeploymentPackage(sourceFile string, destinationFile string) *bytes.Buffer
}

// ScenarioHelper lets the caller specify the path to Lambda handler functions.
type ScenarioHelper struct {
 HandlerPath string
}

// Pause waits for the specified number of seconds.
func (helper *ScenarioHelper) Pause(secs int) {
 time.Sleep(time.Duration(secs) * time.Second)
}
```

```
// CreateDeploymentPackage creates an AWS Lambda deployment package from a source
 file. The
// deployment package is stored in .zip format in a bytes.Buffer. The buffer can
 be
// used to pass a []byte to Lambda when creating the function.
// The specified destinationFile is the name to give the file when it's deployed
 to Lambda.
func (helper *ScenarioHelper) CreateDeploymentPackage(sourceFile string,
 destinationFile string) *bytes.Buffer {
 var err error
 buffer := &bytes.Buffer{}
 writer := zip.NewWriter(buffer)
 zFile, err := writer.Create(destinationFile)
 if err != nil {
  log.Panicf("Couldn't create destination archive %v. Here's why: %v\n",
 destinationFile, err)
 }
 sourceBody, err := os.ReadFile(fmt.Sprintf("%v/%v", helper.HandlerPath,
 sourceFile))
 if err != nil {
  log.Panicf("Couldn't read handler source file %v. Here's why: %v\n",
   sourceFile, err)
 } else {
  _, err = zFile.Write(sourceBody)
  if err != nil {
   log.Panicf("Couldn't write handler %v to zip archive. Here's why: %v\n",
    sourceFile, err)
  }
 }
 err = writer.Close()
 if err != nil {
  log.Panicf("Couldn't close zip writer. Here's why: %v\n", err)
 }
 return buffer
}
```

Créez une structure qui englobe les actions Lambda individuelles.

```
import (
```

```
 "bytes"
 "context"
 "encoding/json"
 "errors"
 "log"
 "time"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/service/lambda"
 "github.com/aws/aws-sdk-go-v2/service/lambda/types"
)

// FunctionWrapper encapsulates function actions used in the examples.
// It contains an AWS Lambda service client that is used to perform user actions.
type FunctionWrapper struct {
 LambdaClient *lambda.Client
}


// GetFunction gets data about the Lambda function specified by functionName.
func (wrapper FunctionWrapper) GetFunction(ctx context.Context, functionName
 string) types.State {
 var state types.State
 funcOutput, err := wrapper.LambdaClient.GetFunction(ctx,
 &lambda.GetFunctionInput{
  FunctionName: aws.String(functionName),
 })
 if err != nil {
  log.Panicf("Couldn't get function %v. Here's why: %v\n", functionName, err)
 } else {
  state = funcOutput.Configuration.State
 }
 return state
}



// CreateFunction creates a new Lambda function from code contained in the
 zipPackage
// buffer. The specified handlerName must match the name of the file and function
// contained in the uploaded code. The role specified by iamRoleArn is assumed by
// Lambda and grants specific permissions.
// When the function already exists, types.StateActive is returned.
```

```
// When the function is created, a lambda.FunctionActiveV2Waiter is used to wait
 until the
// function is active.
func (wrapper FunctionWrapper) CreateFunction(ctx context.Context, functionName
 string, handlerName string,
 iamRoleArn *string, zipPackage *bytes.Buffer) types.State {
 var state types.State
 _, err := wrapper.LambdaClient.CreateFunction(ctx, &lambda.CreateFunctionInput{
  Code:         &types.FunctionCode{ZipFile: zipPackage.Bytes()},
  FunctionName: aws.String(functionName),
  Role:         iamRoleArn,
  Handler:      aws.String(handlerName),
  Publish:      true,
  Runtime:      types.RuntimePython39,
 })
 if err != nil {
  var resConflict *types.ResourceConflictException
  if errors.As(err, &resConflict) {
   log.Printf("Function %v already exists.\n", functionName)
   state = types.StateActive
  } else {
   log.Panicf("Couldn't create function %v. Here's why: %v\n", functionName, err)
  }
 } else {
  waiter := lambda.NewFunctionActiveV2Waiter(wrapper.LambdaClient)
  funcOutput, err := waiter.WaitForOutput(ctx, &lambda.GetFunctionInput{
   FunctionName: aws.String(functionName)}, 1*time.Minute)
  if err != nil {
   log.Panicf("Couldn't wait for function %v to be active. Here's why: %v\n",
 functionName, err)
  } else {
   state = funcOutput.Configuration.State
  }
 }
 return state
}



// UpdateFunctionCode updates the code for the Lambda function specified by
 functionName.
// The existing code for the Lambda function is entirely replaced by the code in
 the
```

```
// zipPackage buffer. After the update action is called, a
 lambda.FunctionUpdatedV2Waiter
// is used to wait until the update is successful.
func (wrapper FunctionWrapper) UpdateFunctionCode(ctx context.Context,
 functionName string, zipPackage *bytes.Buffer) types.State {
 var state types.State
 _, err := wrapper.LambdaClient.UpdateFunctionCode(ctx,
 &lambda.UpdateFunctionCodeInput{
  FunctionName: aws.String(functionName), ZipFile: zipPackage.Bytes(),
 })
 if err != nil {
  log.Panicf("Couldn't update code for function %v. Here's why: %v\n",
 functionName, err)
 } else {
  waiter := lambda.NewFunctionUpdatedV2Waiter(wrapper.LambdaClient)
  funcOutput, err := waiter.WaitForOutput(ctx, &lambda.GetFunctionInput{
   FunctionName: aws.String(functionName)}, 1*time.Minute)
  if err != nil {
   log.Panicf("Couldn't wait for function %v to be active. Here's why: %v\n",
 functionName, err)
  } else {
   state = funcOutput.Configuration.State
  }
 }
 return state
}



// UpdateFunctionConfiguration updates a map of environment variables configured
 for
// the Lambda function specified by functionName.
func (wrapper FunctionWrapper) UpdateFunctionConfiguration(ctx context.Context,
 functionName string, envVars map[string]string) {
 _, err := wrapper.LambdaClient.UpdateFunctionConfiguration(ctx,
 &lambda.UpdateFunctionConfigurationInput{
  FunctionName: aws.String(functionName),
  Environment:  &types.Environment{Variables: envVars},
 })
 if err != nil {
  log.Panicf("Couldn't update configuration for %v. Here's why: %v",
 functionName, err)
 }
}
```

```
// ListFunctions lists up to maxItems functions for the account. This function
 uses a
// lambda.ListFunctionsPaginator to paginate the results.
func (wrapper FunctionWrapper) ListFunctions(ctx context.Context, maxItems int)
 []types.FunctionConfiguration {
 var functions []types.FunctionConfiguration
 paginator := lambda.NewListFunctionsPaginator(wrapper.LambdaClient,
 &lambda.ListFunctionsInput{
  MaxItems: aws.Int32(int32(maxItems)),
 })
 for paginator.HasMorePages() && len(functions) < maxItems {
  pageOutput, err := paginator.NextPage(ctx)
  if err != nil {
   log.Panicf("Couldn't list functions for your account. Here's why: %v\n", err)
  }
  functions = append(functions, pageOutput.Functions...)
 }
 return functions
}



// DeleteFunction deletes the Lambda function specified by functionName.
func (wrapper FunctionWrapper) DeleteFunction(ctx context.Context, functionName
 string) {
 _, err := wrapper.LambdaClient.DeleteFunction(ctx, &lambda.DeleteFunctionInput{
  FunctionName: aws.String(functionName),
 })
 if err != nil {
  log.Panicf("Couldn't delete function %v. Here's why: %v\n", functionName, err)
 }
}



// Invoke invokes the Lambda function specified by functionName, passing the
 parameters
// as a JSON payload. When getLog is true, types.LogTypeTail is specified, which
 tells
// Lambda to include the last few log lines in the returned result.
```

```
func (wrapper FunctionWrapper) Invoke(ctx context.Context, functionName string,
 parameters any, getLog bool) *lambda.InvokeOutput {
 logType := types.LogTypeNone
 if getLog {
  logType = types.LogTypeTail
 }
 payload, err := json.Marshal(parameters)
 if err != nil {
  log.Panicf("Couldn't marshal parameters to JSON. Here's why %v\n", err)
 }
 invokeOutput, err := wrapper.LambdaClient.Invoke(ctx, &lambda.InvokeInput{
  FunctionName: aws.String(functionName),
  LogType:      logType,
  Payload:      payload,
 })
 if err != nil {
  log.Panicf("Couldn't invoke function %v. Here's why: %v\n", functionName, err)
 }
 return invokeOutput
}



// IncrementParameters is used to serialize parameters to the increment Lambda
 handler.
type IncrementParameters struct {
 Action string `json:"action"`
 Number int    `json:"number"`
}

// CalculatorParameters is used to serialize parameters to the calculator Lambda
 handler.
type CalculatorParameters struct {
 Action string `json:"action"`
 X      int    `json:"x"`
 Y      int    `json:"y"`
}

// LambdaResultInt is used to deserialize an int result from a Lambda handler.
type LambdaResultInt struct {
 Result int `json:"result"`
}
```

```
// LambdaResultFloat is used to deserialize a float32 result from a Lambda
 handler.
type LambdaResultFloat struct {
 Result float32 `json:"result"`
}
```

Définir un gestionnaire Lambda qui incrémente un nombre.

```
import logging

logger = logging.getLogger()
logger.setLevel(logging.INFO)


def lambda_handler(event, context):
    """
    Accepts an action and a single number, performs the specified action on the
 number,
    and returns the result. The only allowable action is 'increment'.

    :param event: The event dict that contains the parameters sent when the
 function
                  is invoked.
    :param context: The context in which the function is called.
    :return: The result of the action.
    """
    result = None
    action = event.get("action")
    if action == "increment":
        result = event.get("number", 0) + 1
        logger.info("Calculated result of %s", result)
    else:
        logger.error("%s is not a valid action.", action)

    response = {"result": result}
    return response
```

Définir un deuxième gestionnaire Lambda qui effectue des opérations arithmétiques.

```
import logging
import os


logger = logging.getLogger()

# Define a list of Python lambda functions that are called by this AWS Lambda
 function.
ACTIONS = {
    "plus": lambda x, y: x + y,
    "minus": lambda x, y: x - y,
    "times": lambda x, y: x * y,
    "divided-by": lambda x, y: x / y,
}


def lambda_handler(event, context):
    """
    Accepts an action and two numbers, performs the specified action on the
 numbers,
    and returns the result.

    :param event: The event dict that contains the parameters sent when the
 function
                  is invoked.
    :param context: The context in which the function is called.
    :return: The result of the specified action.
    """
    # Set the log level based on a variable configured in the Lambda environment.
    logger.setLevel(os.environ.get("LOG_LEVEL", logging.INFO))
    logger.debug("Event: %s", event)

    action = event.get("action")
    func = ACTIONS.get(action)
    x = event.get("x")
    y = event.get("y")
    result = None
    try:
        if func is not None and x is not None and y is not None:
            result = func(x, y)
            logger.info("%s %s %s is %s", x, action, y, result)
        else:
            logger.error("I can't calculate %s %s %s.", x, action, y)
```

```
    except ZeroDivisionError:
        logger.warning("I can't divide %s by 0!", x)

    response = {"result": result}
    return response
```

- Pour plus d'informations sur l'API, consultez les rubriques suivantes dans la référence de l'API AWS SDK pour Go .
  - CreateFunction
  - DeleteFunction
  - GetFunction
  - Invoke
  - ListFunctions
  - UpdateFunctionCode
  - UpdateFunctionConfiguration

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
/*
 *  Lambda function names appear as:
 *
 *  arn:aws:lambda:us-west-2:335556666777:function:HelloFunction
 *
 *  To find this value, look at the function in the AWS Management Console.
 *
 *  Before running this Java code example, set up your development environment,
 including your credentials.
```

```
 *
 *  For more information, see this documentation topic:
 *
 *  https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 *
 *  This example performs the following tasks:
 *
 * 1. Creates an AWS Lambda function.
 * 2. Gets a specific AWS Lambda function.
 * 3. Lists all Lambda functions.
 * 4. Invokes a Lambda function.
 * 5. Updates the Lambda function code and invokes it again.
 * 6. Updates a Lambda function's configuration value.
 * 7. Deletes a Lambda function.
 */

public class LambdaScenario {
    public static final String DASHES = new String(new char[80]).replace("\0",
 "-");

    public static void main(String[] args) throws InterruptedException {
        final String usage = """

            Usage:
                <functionName> <role> <handler> <bucketName> <key>\s

            Where:
                functionName - The name of the Lambda function.\s
                role - The AWS Identity and Access Management (IAM) service role
 that has Lambda permissions.\s
                handler - The fully qualified method name (for example,
 example.Handler::handleRequest).\s
                bucketName - The Amazon Simple Storage Service (Amazon S3) bucket
 name that contains the .zip or .jar used to update the Lambda function's code.\s
                key - The Amazon S3 key name that represents the .zip or .jar
 (for example, LambdaHello-1.0-SNAPSHOT.jar).
                """;

        if (args.length != 5) {
              System.out.println(usage);
              return;
        }
```

```
        String functionName = args[0];
        String role = args[1];
        String handler = args[2];
        String bucketName = args[3];
        String key = args[4];
        LambdaClient awsLambda = LambdaClient.builder()
            .build();

        System.out.println(DASHES);
        System.out.println("Welcome to the AWS Lambda Basics scenario.");
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("1. Create an AWS Lambda function.");
        String funArn = createLambdaFunction(awsLambda, functionName, key,
bucketName, role, handler);
        System.out.println("The AWS Lambda ARN is " + funArn);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("2. Get the " + functionName + " AWS Lambda
function.");
        getFunction(awsLambda, functionName);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("3. List all AWS Lambda functions.");
        listFunctions(awsLambda);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("4. Invoke the Lambda function.");
        System.out.println("*** Sleep for 1 min to get Lambda function ready.");
        Thread.sleep(60000);
        invokeFunction(awsLambda, functionName);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("5. Update the Lambda function code and invoke it
again.");
        updateFunctionCode(awsLambda, functionName, bucketName, key);
        System.out.println("*** Sleep for 1 min to get Lambda function ready.");
        Thread.sleep(60000);
        invokeFunction(awsLambda, functionName);
```

```
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("6. Update a Lambda function's configuration value.");
        updateFunctionConfiguration(awsLambda, functionName, handler);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("7. Delete the AWS Lambda function.");
        LambdaScenario.deleteLambdaFunction(awsLambda, functionName);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("The AWS Lambda scenario completed successfully");
        System.out.println(DASHES);
        awsLambda.close();
    }

    /**
     * Creates a new Lambda function in AWS using the AWS Lambda Java API.
     *
     * @param awsLambda    the AWS Lambda client used to interact with the AWS
Lambda service
     * @param functionName the name of the Lambda function to create
     * @param key          the S3 key of the function code
     * @param bucketName   the name of the S3 bucket containing the function code
     * @param role         the IAM role to assign to the Lambda function
     * @param handler      the fully qualified class name of the function handler
     * @return the Amazon Resource Name (ARN) of the created Lambda function
     */
    public static String createLambdaFunction(LambdaClient awsLambda,
                                               String functionName,
                                               String key,
                                               String bucketName,
                                               String role,
                                               String handler) {

        try {
            LambdaWaiter waiter = awsLambda.waiter();
            FunctionCode code = FunctionCode.builder()
                .s3Key(key)
                .s3Bucket(bucketName)
                .build();
```

```
            CreateFunctionRequest functionRequest =
CreateFunctionRequest.builder()
                .functionName(functionName)
                .description("Created by the Lambda Java API")
                .code(code)
                .handler(handler)
                .runtime(Runtime.JAVA17)
                .role(role)
                .build();

            // Create a Lambda function using a waiter
            CreateFunctionResponse functionResponse =
awsLambda.createFunction(functionRequest);
            GetFunctionRequest getFunctionRequest = GetFunctionRequest.builder()
                .functionName(functionName)
                .build();
            WaiterResponse<GetFunctionResponse> waiterResponse =
waiter.waitUntilFunctionExists(getFunctionRequest);
            waiterResponse.matched().response().ifPresent(System.out::println);
            return functionResponse.functionArn();

        } catch (LambdaException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
        return "";
    }

    /**
     * Retrieves information about an AWS Lambda function.
     *
     * @param awsLambda    an instance of the {@link LambdaClient} class, which
is used to interact with the AWS Lambda service
     * @param functionName the name of the AWS Lambda function to retrieve
information about
     */
    public static void getFunction(LambdaClient awsLambda, String functionName) {
        try {
            GetFunctionRequest functionRequest = GetFunctionRequest.builder()
                .functionName(functionName)
                .build();

            GetFunctionResponse response =
awsLambda.getFunction(functionRequest);
```

```
            System.out.println("The runtime of this Lambda function is " +
response.configuration().runtime());

        } catch (LambdaException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }

    /**
     * Lists the AWS Lambda functions associated with the current AWS account.
     *
     * @param awsLambda an instance of the {@link LambdaClient} class, which is
used to interact with the AWS Lambda service
     *
     * @throws LambdaException if an error occurs while interacting with the AWS
Lambda service
     */
    public static void listFunctions(LambdaClient awsLambda) {
        try {
            ListFunctionsResponse functionResult = awsLambda.listFunctions();
            List<FunctionConfiguration> list = functionResult.functions();
            for (FunctionConfiguration config : list) {
                System.out.println("The function name is " +
config.functionName());
            }

        } catch (LambdaException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }

    /**
     * Invokes a specific AWS Lambda function.
     *
     * @param awsLambda    an instance of {@link LambdaClient} to interact with
the AWS Lambda service
     * @param functionName the name of the AWS Lambda function to be invoked
     */
    public static void invokeFunction(LambdaClient awsLambda, String
functionName) {
        InvokeResponse res;
        try {
```

```
            // Need a SdkBytes instance for the payload.
            JSONObject jsonObj = new JSONObject();
            jsonObj.put("inputValue", "2000");
            String json = jsonObj.toString();
            SdkBytes payload = SdkBytes.fromUtf8String(json);

            InvokeRequest request = InvokeRequest.builder()
                .functionName(functionName)
                .payload(payload)
                .build();

            res = awsLambda.invoke(request);
            String value = res.payload().asUtf8String();
            System.out.println(value);

        } catch (LambdaException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }

    /**
     * Updates the code for an AWS Lambda function.
     *
     * @param awsLambda  the AWS Lambda client
     * @param functionName the name of the Lambda function to update
     * @param bucketName the name of the S3 bucket where the function code is
located
     * @param key the key (file name) of the function code in the S3 bucket
     * @throws LambdaException if there is an error updating the function code
     */
    public static void updateFunctionCode(LambdaClient awsLambda, String
functionName, String bucketName, String key) {
        try {
            LambdaWaiter waiter = awsLambda.waiter();
            UpdateFunctionCodeRequest functionCodeRequest =
UpdateFunctionCodeRequest.builder()
                .functionName(functionName)
                .publish(true)
                .s3Bucket(bucketName)
                .s3Key(key)
                .build();
```

```
            UpdateFunctionCodeResponse response =
awsLambda.updateFunctionCode(functionCodeRequest);
            GetFunctionConfigurationRequest getFunctionConfigRequest =
GetFunctionConfigurationRequest.builder()
                .functionName(functionName)
                .build();

            WaiterResponse<GetFunctionConfigurationResponse> waiterResponse =
waiter
                .waitUntilFunctionUpdated(getFunctionConfigRequest);
            waiterResponse.matched().response().ifPresent(System.out::println);
            System.out.println("The last modified value is " +
response.lastModified());

        } catch (LambdaException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }

    /**
     * Updates the configuration of an AWS Lambda function.
     *
     * @param awsLambda     the {@link LambdaClient} instance to use for the AWS
Lambda operation
     * @param functionName  the name of the AWS Lambda function to update
     * @param handler       the new handler for the AWS Lambda function
     *
     * @throws LambdaException if there is an error while updating the function
configuration
     */
    public static void updateFunctionConfiguration(LambdaClient awsLambda, String
functionName, String handler) {
        try {
            UpdateFunctionConfigurationRequest configurationRequest =
UpdateFunctionConfigurationRequest.builder()
                .functionName(functionName)
                .handler(handler)
                .runtime(Runtime.JAVA17)
                .build();

            awsLambda.updateFunctionConfiguration(configurationRequest);

        } catch (LambdaException e) {
```

```
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }

    /**
     * Deletes an AWS Lambda function.
     *
     * @param awsLambda     an instance of the {@link LambdaClient} class, which
 is used to interact with the AWS Lambda service
     * @param functionName  the name of the Lambda function to be deleted
     *
     * @throws LambdaException if an error occurs while deleting the Lambda
 function
     */
    public static void deleteLambdaFunction(LambdaClient awsLambda, String
 functionName) {
        try {
            DeleteFunctionRequest request = DeleteFunctionRequest.builder()
                .functionName(functionName)
                .build();

            awsLambda.deleteFunction(request);
            System.out.println("The " + functionName + " function was deleted");

        } catch (LambdaException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
}
```

- Pour plus de détails sur l'API, consultez les rubriques suivantes dans la Référence des API du kit AWS SDK for Java 2.x .
  - CreateFunction
  - DeleteFunction
  - GetFunction
  - Invoke
  - ListFunctions
  - UpdateFunctionCode

- UpdateFunctionConfiguration

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Créez un Gestion des identités et des accès AWS Rôle (IAM) qui accorde à Lambda l'autorisation d'écrire dans les journaux.

```
    logger.log(`Creating role (${NAME_ROLE_LAMBDA})...`);
    const response = await createRole(NAME_ROLE_LAMBDA);

import { AttachRolePolicyCommand, IAMClient } from "@aws-sdk/client-iam";

const client = new IAMClient({});

/**
 *
 * @param {string} policyArn
 * @param {string} roleName
 */
export const attachRolePolicy = (policyArn, roleName) => {
  const command = new AttachRolePolicyCommand({
    PolicyArn: policyArn,
    RoleName: roleName,
  });

  return client.send(command);
};
```

Créer une fonction Lambda et télécharger le code de gestionnaire.

```
const createFunction = async (funcName, roleArn) => {
  const client = new LambdaClient({});
```

```
  const code = await readFile(`${dirname}../functions/${funcName}.zip`);

  const command = new CreateFunctionCommand({
    Code: { ZipFile: code },
    FunctionName: funcName,
    Role: roleArn,
    Architectures: [Architecture.arm64],
    Handler: "index.handler", // Required when sending a .zip file
    PackageType: PackageType.Zip, // Required when sending a .zip file
    Runtime: Runtime.nodejs16x, // Required when sending a .zip file
  });

  return client.send(command);
};
```

Invoquer la fonction avec un seul paramètre et obtenir des résultats.

```
const invoke = async (funcName, payload) => {
  const client = new LambdaClient({});
  const command = new InvokeCommand({
    FunctionName: funcName,
    Payload: JSON.stringify(payload),
    LogType: LogType.Tail,
  });

  const { Payload, LogResult } = await client.send(command);
  const result = Buffer.from(Payload).toString();
  const logs = Buffer.from(LogResult, "base64").toString();
  return { logs, result };
};
```

Mettre à jour le code de fonction et configurer son environnement Lambda avec une variable d'environnement.

```
const updateFunctionCode = async (funcName, newFunc) => {
  const client = new LambdaClient({});
  const code = await readFile(`${dirname}../functions/${newFunc}.zip`);
  const command = new UpdateFunctionCodeCommand({
    ZipFile: code,
    FunctionName: funcName,
    Architectures: [Architecture.arm64],
```

```
    Handler: "index.handler", // Required when sending a .zip file
    PackageType: PackageType.Zip, // Required when sending a .zip file
    Runtime: Runtime.nodejs16x, // Required when sending a .zip file
  });

  return client.send(command);
};

const updateFunctionConfiguration = async (funcName) => {
  const client = new LambdaClient({});
  const config = readFileSync(`${dirname}../functions/config.json`).toString();
  const command = new UpdateFunctionConfigurationCommand({
    ...JSON.parse(config),
    FunctionName: funcName,
  });
  const result = await client.send(command);
  await waitForFunctionUpdated({ FunctionName: funcName });
  return result;
};
```

Répertorier les fonctions pour votre compte.

```
const listFunctions = () => {
  const client = new LambdaClient({});
  const command = new ListFunctionsCommand({});

  return client.send(command);
};
```

Supprimer le rôle IAM et la fonction Lambda.

```
import { DeleteRoleCommand, IAMClient } from "@aws-sdk/client-iam";

const client = new IAMClient({});

/**
 *
 * @param {string} roleName
 */
export const deleteRole = (roleName) => {
  const command = new DeleteRoleCommand({ RoleName: roleName });
```

```
  return client.send(command);
};

/**
 * @param {string} funcName
 */
const deleteFunction = (funcName) => {
  const client = new LambdaClient({});
  const command = new DeleteFunctionCommand({ FunctionName: funcName });
  return client.send(command);
};
```

- Pour plus d'informations sur l'API, consultez les rubriques suivantes dans la référence de l'API AWS SDK pour JavaScript .
  - CreateFunction
  - DeleteFunction
  - GetFunction
  - Invoke
  - ListFunctions
  - UpdateFunctionCode
  - UpdateFunctionConfiguration

Kotlin

SDK pour Kotlin

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
suspend fun main(args: Array<String>) {
    val usage = """
        Usage:
            <functionName> <role> <handler> <bucketName> <updatedBucketName>
 <key>
```

```
        Where:
            functionName - The name of the AWS Lambda function.
            role - The AWS Identity and Access Management (IAM) service role that
has AWS Lambda permissions.
            handler - The fully qualified method name (for example,
example.Handler::handleRequest).
            bucketName - The Amazon Simple Storage Service (Amazon S3) bucket
name that contains the ZIP or JAR used for the Lambda function's code.
            updatedBucketName - The Amazon S3 bucket name that contains the .zip
or .jar used to update the Lambda function's code.
            key - The Amazon S3 key name that represents the .zip or .jar file
(for example, LambdaHello-1.0-SNAPSHOT.jar).
            """

    if (args.size != 6) {
        println(usage)
        exitProcess(1)
    }

    val functionName = args[0]
    val role = args[1]
    val handler = args[2]
    val bucketName = args[3]
    val updatedBucketName = args[4]
    val key = args[5]

    println("Creating a Lambda function named $functionName.")
    val funArn = createScFunction(functionName, bucketName, key, handler, role)
    println("The AWS Lambda ARN is $funArn")

    // Get a specific Lambda function.
    println("Getting the $functionName AWS Lambda function.")
    getFunction(functionName)

    // List the Lambda functions.
    println("Listing all AWS Lambda functions.")
    listFunctionsSc()

    // Invoke the Lambda function.
    println("*** Invoke the Lambda function.")
    invokeFunctionSc(functionName)

    // Update the AWS Lambda function code.
```

```
    println("*** Update the Lambda function code.")
    updateFunctionCode(functionName, updatedBucketName, key)

    // println("*** Invoke the function again after updating the code.")
    invokeFunctionSc(functionName)

    // Update the AWS Lambda function configuration.
    println("Update the run time of the function.")
    updateFunctionConfiguration(functionName, handler)

    // Delete the AWS Lambda function.
    println("Delete the AWS Lambda function.")
    delFunction(functionName)
}

suspend fun createScFunction(
    myFunctionName: String,
    s3BucketName: String,
    myS3Key: String,
    myHandler: String,
    myRole: String,
): String {
    val functionCode =
        FunctionCode {
            s3Bucket = s3BucketName
            s3Key = myS3Key
        }

    val request =
        CreateFunctionRequest {
            functionName = myFunctionName
            code = functionCode
            description = "Created by the Lambda Kotlin API"
            handler = myHandler
            role = myRole
            runtime = Runtime.Java17
        }

    // Create a Lambda function using a waiter
    LambdaClient { region = "us-east-1" }.use { awsLambda ->
        val functionResponse = awsLambda.createFunction(request)
        awsLambda.waitUntilFunctionActive {
            functionName = myFunctionName
        }
```

```
        return functionResponse.functionArn.toString()
    }
}

suspend fun getFunction(functionNameVal: String) {
    val functionRequest =
        GetFunctionRequest {
            functionName = functionNameVal
        }

    LambdaClient { region = "us-east-1" }.use { awsLambda ->
        val response = awsLambda.getFunction(functionRequest)
        println("The runtime of this Lambda function is
 ${response.configuration?.runtime}")
    }
}

suspend fun listFunctionsSc() {
    val request =
        ListFunctionsRequest {
            maxItems = 10
        }

    LambdaClient { region = "us-east-1" }.use { awsLambda ->
        val response = awsLambda.listFunctions(request)
        response.functions?.forEach { function ->
            println("The function name is ${function.functionName}")
        }
    }
}

suspend fun invokeFunctionSc(functionNameVal: String) {
    val json = """{"inputValue":"1000"}"""
    val byteArray = json.trimIndent().encodeToByteArray()
    val request =
        InvokeRequest {
            functionName = functionNameVal
            payload = byteArray
            logType = LogType.Tail
        }

    LambdaClient { region = "us-east-1" }.use { awsLambda ->
        val res = awsLambda.invoke(request)
```

```
        println("The function payload is
 ${res.payload?.toString(Charsets.UTF_8)}")
    }
}

suspend fun updateFunctionCode(
    functionNameVal: String?,
    bucketName: String?,
    key: String?,
) {
    val functionCodeRequest =
        UpdateFunctionCodeRequest {
            functionName = functionNameVal
            publish = true
            s3Bucket = bucketName
            s3Key = key
        }

    LambdaClient { region = "us-east-1" }.use { awsLambda ->
        val response = awsLambda.updateFunctionCode(functionCodeRequest)
        awsLambda.waitUntilFunctionUpdated {
            functionName = functionNameVal
        }
        println("The last modified value is " + response.lastModified)
    }
}

suspend fun updateFunctionConfiguration(
    functionNameVal: String?,
    handlerVal: String?,
) {
    val configurationRequest =
        UpdateFunctionConfigurationRequest {
            functionName = functionNameVal
            handler = handlerVal
            runtime = Runtime.Java17
        }

    LambdaClient { region = "us-east-1" }.use { awsLambda ->
        awsLambda.updateFunctionConfiguration(configurationRequest)
    }
}

suspend fun delFunction(myFunctionName: String) {
```

```
    val request =
        DeleteFunctionRequest {
            functionName = myFunctionName
        }

    LambdaClient { region = "us-east-1" }.use { awsLambda ->
        awsLambda.deleteFunction(request)
        println("$myFunctionName was deleted")
    }
}
```

- Pour plus de détails sur l'API, consultez les rubriques suivantes dans la Référence des API du kit AWS SDK pour Kotlin.
  - CreateFunction
  - DeleteFunction
  - GetFunction
  - Invoke
  - ListFunctions
  - UpdateFunctionCode
  - UpdateFunctionConfiguration

PHP

Kit SDK pour PHP

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
namespace Lambda;

use Aws\S3\S3Client;
use GuzzleHttp\Psr7\Stream;
use Iam\IAMService;
```

```
class GettingStartedWithLambda
{
    public function run()
    {
        echo("\n");
        echo("---------------------------------------\n");
        print("Welcome to the AWS Lambda getting started demo using PHP!\n");
        echo("---------------------------------------\n");

        $clientArgs = [
            'region' => 'us-west-2',
            'version' => 'latest',
            'profile' => 'default',
        ];
        $uniqid = uniqid();

        $iamService = new IAMService();
        $s3client = new S3Client($clientArgs);
        $lambdaService = new LambdaService();

        echo "First, let's create a role to run our Lambda code.\n";
        $roleName = "test-lambda-role-$uniqid";
        $rolePolicyDocument = "{
            \"Version\": \"2012-10-17\",
            \"Statement\": [
                {
                    \"Effect\": \"Allow\",
                    \"Principal\": {
                        \"Service\": \"lambda.amazonaws.com\"
                    },
                    \"Action\": \"sts:AssumeRole\"
                }
            ]
        }";
        $role = $iamService->createRole($roleName, $rolePolicyDocument);
        echo "Created role {$role['RoleName']}.\n";

        $iamService->attachRolePolicy(
            $role['RoleName'],
            "arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole"
        );
        echo "Attached the AWSLambdaBasicExecutionRole to {$role['RoleName']}.
\n";
```

```
        echo "\nNow let's create an S3 bucket and upload our Lambda code there.
\n";
        $bucketName = "amzn-s3-demo-bucket-$uniqid";
        $s3client->createBucket([
            'Bucket' => $bucketName,
        ]);
        echo "Created bucket $bucketName.\n";

        $functionName = "doc_example_lambda_$uniqid";
        $codeBasic = __DIR__ . "/lambda_handler_basic.zip";
        $handler = "lambda_handler_basic";
        $file = file_get_contents($codeBasic);
        $s3client->putObject([
            'Bucket' => $bucketName,
            'Key' => $functionName,
            'Body' => $file,
        ]);
        echo "Uploaded the Lambda code.\n";

        $createLambdaFunction = $lambdaService->createFunction($functionName,
 $role, $bucketName, $handler);
        // Wait until the function has finished being created.
        do {
            $getLambdaFunction = $lambdaService-
>getFunction($createLambdaFunction['FunctionName']);
        } while ($getLambdaFunction['Configuration']['State'] == "Pending");
        echo "Created Lambda function {$getLambdaFunction['Configuration']
['FunctionName']}.\n";

        sleep(1);

        echo "\nOk, let's invoke that Lambda code.\n";
        $basicParams = [
            'action' => 'increment',
            'number' => 3,
        ];
        /** @var Stream $invokeFunction */
        $invokeFunction = $lambdaService->invoke($functionName, $basicParams)
['Payload'];
        $result = json_decode($invokeFunction->getContents())->result;
        echo "After invoking the Lambda code with the input of
 {$basicParams['number']} we received $result.\n";

        echo "\nSince that's working, let's update the Lambda code.\n";
```

```
        $codeCalculator = "lambda_handler_calculator.zip";
        $handlerCalculator = "lambda_handler_calculator";
        echo "First, put the new code into the S3 bucket.\n";
        $file = file_get_contents($codeCalculator);
        $s3client->putObject([
            'Bucket' => $bucketName,
            'Key' => $functionName,
            'Body' => $file,
        ]);
        echo "New code uploaded.\n";

        $lambdaService->updateFunctionCode($functionName, $bucketName,
 $functionName);
        // Wait for the Lambda code to finish updating.
        do {
            $getLambdaFunction = $lambdaService-
>getFunction($createLambdaFunction['FunctionName']);
        } while ($getLambdaFunction['Configuration']['LastUpdateStatus'] !==
 "Successful");
        echo "New Lambda code uploaded.\n";

        $environment = [
            'Variable' => ['Variables' => ['LOG_LEVEL' => 'DEBUG']],
        ];
        $lambdaService->updateFunctionConfiguration($functionName,
 $handlerCalculator, $environment);
        do {
            $getLambdaFunction = $lambdaService-
>getFunction($createLambdaFunction['FunctionName']);
        } while ($getLambdaFunction['Configuration']['LastUpdateStatus'] !==
 "Successful");
        echo "Lambda code updated with new handler and a LOG_LEVEL of DEBUG for
 more information.\n";

        echo "Invoke the new code with some new data.\n";
        $calculatorParams = [
            'action' => 'plus',
            'x' => 5,
            'y' => 4,
        ];
        $invokeFunction = $lambdaService->invoke($functionName,
 $calculatorParams, "Tail");
        $result = json_decode($invokeFunction['Payload']->getContents())->result;
```

```
        echo "Indeed, {$calculatorParams['x']} + {$calculatorParams['y']} does
equal $result.\n";
        echo "Here's the extra debug info: ";
        echo base64_decode($invokeFunction['LogResult']) . "\n";

        echo "\nBut what happens if you try to divide by zero?\n";
        $divZeroParams = [
            'action' => 'divide',
            'x' => 5,
            'y' => 0,
        ];
        $invokeFunction = $lambdaService->invoke($functionName, $divZeroParams,
"Tail");
        $result = json_decode($invokeFunction['Payload']->getContents())->result;
        echo "You get a |$result| result.\n";
        echo "And an error message: ";
        echo base64_decode($invokeFunction['LogResult']) . "\n";

        echo "\nHere's all the Lambda functions you have in this Region:\n";
        $listLambdaFunctions = $lambdaService->listFunctions(5);
        $allLambdaFunctions = $listLambdaFunctions['Functions'];
        $next = $listLambdaFunctions->get('NextMarker');
        while ($next != false) {
            $listLambdaFunctions = $lambdaService->listFunctions(5, $next);
            $next = $listLambdaFunctions->get('NextMarker');
            $allLambdaFunctions = array_merge($allLambdaFunctions,
$listLambdaFunctions['Functions']);
        }
        foreach ($allLambdaFunctions as $function) {
            echo "{$function['FunctionName']}\n";
        }

        echo "\n\nAnd don't forget to clean up your data!\n";

        $lambdaService->deleteFunction($functionName);
        echo "Deleted Lambda function.\n";
        $iamService->deleteRole($role['RoleName']);
        echo "Deleted Role.\n";
        $deleteObjects = $s3client->listObjectsV2([
            'Bucket' => $bucketName,
        ]);
        $deleteObjects = $s3client->deleteObjects([
            'Bucket' => $bucketName,
            'Delete' => [
```

```
                'Objects' => $deleteObjects['Contents'],
            ]
        ]);
        echo "Deleted all objects from the S3 bucket.\n";
        $s3client->deleteBucket(['Bucket' => $bucketName]);
        echo "Deleted the bucket.\n";
    }
}
```

- Pour plus de détails sur l'API, consultez les rubriques suivantes dans la Référence des API du kit AWS SDK pour PHP .
  - CreateFunction
  - DeleteFunction
  - GetFunction
  - Invoke
  - ListFunctions
  - UpdateFunctionCode
  - UpdateFunctionConfiguration

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Définir un gestionnaire Lambda qui incrémente un nombre.

```
import logging

logger = logging.getLogger()
logger.setLevel(logging.INFO)
```

```
def lambda_handler(event, context):
    """
    Accepts an action and a single number, performs the specified action on the
 number,
    and returns the result. The only allowable action is 'increment'.

    :param event: The event dict that contains the parameters sent when the
 function
                  is invoked.
    :param context: The context in which the function is called.
    :return: The result of the action.
    """
    result = None
    action = event.get("action")
    if action == "increment":
        result = event.get("number", 0) + 1
        logger.info("Calculated result of %s", result)
    else:
        logger.error("%s is not a valid action.", action)

    response = {"result": result}
    return response
```

Définir un deuxième gestionnaire Lambda qui effectue des opérations arithmétiques.

```
import logging
import os


logger = logging.getLogger()

# Define a list of Python lambda functions that are called by this AWS Lambda
 function.
ACTIONS = {
    "plus": lambda x, y: x + y,
    "minus": lambda x, y: x - y,
    "times": lambda x, y: x * y,
    "divided-by": lambda x, y: x / y,
}
```

```
def lambda_handler(event, context):
    """
    Accepts an action and two numbers, performs the specified action on the
 numbers,
    and returns the result.

    :param event: The event dict that contains the parameters sent when the
 function
                  is invoked.
    :param context: The context in which the function is called.
    :return: The result of the specified action.
    """
    # Set the log level based on a variable configured in the Lambda environment.
    logger.setLevel(os.environ.get("LOG_LEVEL", logging.INFO))
    logger.debug("Event: %s", event)

    action = event.get("action")
    func = ACTIONS.get(action)
    x = event.get("x")
    y = event.get("y")
    result = None
    try:
        if func is not None and x is not None and y is not None:
            result = func(x, y)
            logger.info("%s %s %s is %s", x, action, y, result)
        else:
            logger.error("I can't calculate %s %s %s.", x, action, y)
    except ZeroDivisionError:
        logger.warning("I can't divide %s by 0!", x)

    response = {"result": result}
    return response
```

Créer des fonctions qui enveloppent les actions Lambda.

```
class LambdaWrapper:
    def __init__(self, lambda_client, iam_resource):
        self.lambda_client = lambda_client
        self.iam_resource = iam_resource
```

```
    @staticmethod
    def create_deployment_package(source_file, destination_file):
        """
        Creates a Lambda deployment package in .zip format in an in-memory
buffer. This
        buffer can be passed directly to Lambda when creating the function.

        :param source_file: The name of the file that contains the Lambda handler
                            function.
        :param destination_file: The name to give the file when it's deployed to
Lambda.
        :return: The deployment package.
        """
        buffer = io.BytesIO()
        with zipfile.ZipFile(buffer, "w") as zipped:
            zipped.write(source_file, destination_file)
        buffer.seek(0)
        return buffer.read()

    def get_iam_role(self, iam_role_name):
        """
        Get an AWS Identity and Access Management (IAM) role.

        :param iam_role_name: The name of the role to retrieve.
        :return: The IAM role.
        """
        role = None
        try:
            temp_role = self.iam_resource.Role(iam_role_name)
            temp_role.load()
            role = temp_role
            logger.info("Got IAM role %s", role.name)
        except ClientError as err:
            if err.response["Error"]["Code"] == "NoSuchEntity":
                logger.info("IAM role %s does not exist.", iam_role_name)
            else:
                logger.error(
                    "Couldn't get IAM role %s. Here's why: %s: %s",
                    iam_role_name,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
```

```
                raise
        return role

    def create_iam_role_for_lambda(self, iam_role_name):
        """
        Creates an IAM role that grants the Lambda function basic permissions. If
a
        role with the specified name already exists, it is used for the demo.

        :param iam_role_name: The name of the role to create.
        :return: The role and a value that indicates whether the role is newly
created.
        """
        role = self.get_iam_role(iam_role_name)
        if role is not None:
            return role, False

        lambda_assume_role_policy = {
            "Version":"2012-10-17",
            "Statement": [
                {
                    "Effect": "Allow",
                    "Principal": {"Service": "lambda.amazonaws.com"},
                    "Action": "sts:AssumeRole",
                }
            ],
        }
        policy_arn = "arn:aws:iam::aws:policy/service-role/
AWSLambdaBasicExecutionRole"

        try:
            role = self.iam_resource.create_role(
                RoleName=iam_role_name,
                AssumeRolePolicyDocument=json.dumps(lambda_assume_role_policy),
            )
            logger.info("Created role %s.", role.name)
            role.attach_policy(PolicyArn=policy_arn)
            logger.info("Attached basic execution policy to role %s.", role.name)
        except ClientError as error:
            if error.response["Error"]["Code"] == "EntityAlreadyExists":
                role = self.iam_resource.Role(iam_role_name)
                logger.warning("The role %s already exists. Using it.",
iam_role_name)
            else:
```

```
                logger.exception(
                    "Couldn't create role %s or attach policy %s.",
                    iam_role_name,
                    policy_arn,
                )
                raise

        return role, True

    def get_function(self, function_name):
        """
        Gets data about a Lambda function.

        :param function_name: The name of the function.
        :return: The function data.
        """
        response = None
        try:
            response =
self.lambda_client.get_function(FunctionName=function_name)
        except ClientError as err:
            if err.response["Error"]["Code"] == "ResourceNotFoundException":
                logger.info("Function %s does not exist.", function_name)
            else:
                logger.error(
                    "Couldn't get function %s. Here's why: %s: %s",
                    function_name,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        return response


    def create_function(
        self, function_name, handler_name, iam_role, deployment_package
    ):
        """
        Deploys a Lambda function.

        :param function_name: The name of the Lambda function.
        :param handler_name: The fully qualified name of the handler function.
This
                             must include the file name and the function name.
```

```
        :param iam_role: The IAM role to use for the function.
        :param deployment_package: The deployment package that contains the
function
                                   code in .zip format.
        :return: The Amazon Resource Name (ARN) of the newly created function.
        """
        try:
            response = self.lambda_client.create_function(
                FunctionName=function_name,
                Description="AWS Lambda doc example",
                Runtime="python3.9",
                Role=iam_role.arn,
                Handler=handler_name,
                Code={"ZipFile": deployment_package},
                Publish=True,
            )
            function_arn = response["FunctionArn"]
            waiter = self.lambda_client.get_waiter("function_active_v2")
            waiter.wait(FunctionName=function_name)
            logger.info(
                "Created function '%s' with ARN: '%s'.",
                function_name,
                response["FunctionArn"],
            )
        except ClientError:
            logger.error("Couldn't create function %s.", function_name)
            raise
        else:
            return function_arn


    def delete_function(self, function_name):
        """
        Deletes a Lambda function.

        :param function_name: The name of the function to delete.
        """
        try:
            self.lambda_client.delete_function(FunctionName=function_name)
        except ClientError:
            logger.exception("Couldn't delete function %s.", function_name)
            raise
```

```
    def invoke_function(self, function_name, function_params, get_log=False):
        """
        Invokes a Lambda function.

        :param function_name: The name of the function to invoke.
        :param function_params: The parameters of the function as a dict. This
dict
                                is serialized to JSON before it is sent to
Lambda.
        :param get_log: When true, the last 4 KB of the execution log are
included in
                        the response.
        :return: The response from the function invocation.
        """
        try:
            response = self.lambda_client.invoke(
                FunctionName=function_name,
                Payload=json.dumps(function_params),
                LogType="Tail" if get_log else "None",
            )
            logger.info("Invoked function %s.", function_name)
        except ClientError:
            logger.exception("Couldn't invoke function %s.", function_name)
            raise
        return response


    def update_function_code(self, function_name, deployment_package):
        """
        Updates the code for a Lambda function by submitting a .zip archive that
contains
        the code for the function.

        :param function_name: The name of the function to update.
        :param deployment_package: The function code to update, packaged as bytes
in
                                   .zip format.
        :return: Data about the update, including the status.
        """
        try:
            response = self.lambda_client.update_function_code(
                FunctionName=function_name, ZipFile=deployment_package
            )
        except ClientError as err:
```

```
            logger.error(
                "Couldn't update function %s. Here's why: %s: %s",
                function_name,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
        else:
            return response


    def update_function_configuration(self, function_name, env_vars):
        """
        Updates the environment variables for a Lambda function.

        :param function_name: The name of the function to update.
        :param env_vars: A dict of environment variables to update.
        :return: Data about the update, including the status.
        """
        try:
            response = self.lambda_client.update_function_configuration(
                FunctionName=function_name, Environment={"Variables": env_vars}
            )
        except ClientError as err:
            logger.error(
                "Couldn't update function configuration %s. Here's why: %s: %s",
                function_name,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
        else:
            return response


    def list_functions(self):
        """
        Lists the Lambda functions for the current account.
        """
        try:
            func_paginator = self.lambda_client.get_paginator("list_functions")
            for func_page in func_paginator.paginate():
                for func in func_page["Functions"]:
                    print(func["FunctionName"])
```

```
                    desc = func.get("Description")
                    if desc:
                        print(f"\t{desc}")
                    print(f"\t{func['Runtime']}: {func['Handler']}")
        except ClientError as err:
            logger.error(
                "Couldn't list functions. Here's why: %s: %s",
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
```

Créer une fonction qui exécute le scénario.

```
class UpdateFunctionWaiter(CustomWaiter):
    """A custom waiter that waits until a function is successfully updated."""

    def __init__(self, client):
        super().__init__(
            "UpdateSuccess",
            "GetFunction",
            "Configuration.LastUpdateStatus",
            {"Successful": WaitState.SUCCESS, "Failed": WaitState.FAILURE},
            client,
        )

    def wait(self, function_name):
        self._wait(FunctionName=function_name)


def run_scenario(lambda_client, iam_resource, basic_file, calculator_file,
 lambda_name):
    """
    Runs the scenario.

    :param lambda_client: A Boto3 Lambda client.
    :param iam_resource: A Boto3 IAM resource.
    :param basic_file: The name of the file that contains the basic Lambda
 handler.
```

```
    :param calculator_file: The name of the file that contains the calculator
Lambda handler.
    :param lambda_name: The name to give resources created for the scenario, such
as the
                        IAM role and the Lambda function.
    """
    logging.basicConfig(level=logging.INFO, format="%(levelname)s: %(message)s")

    print("-" * 88)
    print("Welcome to the AWS Lambda getting started with functions demo.")
    print("-" * 88)

    wrapper = LambdaWrapper(lambda_client, iam_resource)

    print("Checking for IAM role for Lambda...")
    iam_role, should_wait = wrapper.create_iam_role_for_lambda(lambda_name)
    if should_wait:
        logger.info("Giving AWS time to create resources...")
        wait(10)

    print(f"Looking for function {lambda_name}...")
    function = wrapper.get_function(lambda_name)
    if function is None:
        print("Zipping the Python script into a deployment package...")
        deployment_package = wrapper.create_deployment_package(
            basic_file, f"{lambda_name}.py"
        )
        print(f"...and creating the {lambda_name} Lambda function.")
        wrapper.create_function(
            lambda_name, f"{lambda_name}.lambda_handler", iam_role,
deployment_package
        )
    else:
        print(f"Function {lambda_name} already exists.")
    print("-" * 88)

    print(f"Let's invoke {lambda_name}. This function increments a number.")
    action_params = {
        "action": "increment",
        "number": q.ask("Give me a number to increment: ", q.is_int),
    }
    print(f"Invoking {lambda_name}...")
    response = wrapper.invoke_function(lambda_name, action_params)
    print(
```

```
        f"Incrementing {action_params['number']} resulted in "
        f"{json.load(response['Payload'])}"
    )
    print("-" * 88)

    print(f"Let's update the function to an arithmetic calculator.")
    q.ask("Press Enter when you're ready.")
    print("Creating a new deployment package...")
    deployment_package = wrapper.create_deployment_package(
        calculator_file, f"{lambda_name}.py"
    )
    print(f"...and updating the {lambda_name} Lambda function.")
    update_waiter = UpdateFunctionWaiter(lambda_client)
    wrapper.update_function_code(lambda_name, deployment_package)
    update_waiter.wait(lambda_name)
    print(f"This function uses an environment variable to control logging
level.")
    print(f"Let's set it to DEBUG to get the most logging.")
    wrapper.update_function_configuration(
        lambda_name, {"LOG_LEVEL": logging.getLevelName(logging.DEBUG)}
    )

    actions = ["plus", "minus", "times", "divided-by"]
    want_invoke = True
    while want_invoke:
        print(f"Let's invoke {lambda_name}. You can invoke these actions:")
        for index, action in enumerate(actions):
            print(f"{index + 1}: {action}")
        action_params = {}
        action_index = q.ask(
            "Enter the number of the action you want to take: ",
            q.is_int,
            q.in_range(1, len(actions)),
        )
        action_params["action"] = actions[action_index - 1]
        print(f"You've chosen to invoke 'x {action_params['action']} y'.")
        action_params["x"] = q.ask("Enter a value for x: ", q.is_int)
        action_params["y"] = q.ask("Enter a value for y: ", q.is_int)
        print(f"Invoking {lambda_name}...")
        response = wrapper.invoke_function(lambda_name, action_params, True)
        print(
            f"Calculating {action_params['x']} {action_params['action']}
{action_params['y']} "
            f"resulted in {json.load(response['Payload'])}"
```

```
        )
        q.ask("Press Enter to see the logs from the call.")
        print(base64.b64decode(response["LogResult"]).decode())
        want_invoke = q.ask("That was fun. Shall we do it again? (y/n) ",
 q.is_yesno)
    print("-" * 88)

    if q.ask(
        "Do you want to list all of the functions in your account? (y/n) ",
 q.is_yesno
    ):
        wrapper.list_functions()
    print("-" * 88)

    if q.ask("Ready to delete the function and role? (y/n) ", q.is_yesno):
        for policy in iam_role.attached_policies.all():
            policy.detach_role(RoleName=iam_role.name)
        iam_role.delete()
        print(f"Deleted role {lambda_name}.")
        wrapper.delete_function(lambda_name)
        print(f"Deleted function {lambda_name}.")

    print("\nThanks for watching!")
    print("-" * 88)


if __name__ == "__main__":
    try:
        run_scenario(
            boto3.client("lambda"),
            boto3.resource("iam"),
            "lambda_handler_basic.py",
            "lambda_handler_calculator.py",
            "doc_example_lambda_calculator",
        )
    except Exception:
        logging.exception("Something went wrong with the demo!")
```

- Pour plus d'informations sur l'API, consultez les rubriques suivantes dans AWS SDK for Python (Boto3) API Reference.
  - CreateFunction

- DeleteFunction
- GetFunction
- Invoke
- ListFunctions
- UpdateFunctionCode
- UpdateFunctionConfiguration

Ruby

Kit SDK pour Ruby

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Configurez les autorisations IAM préalables pour une fonction Lambda capable d'écrire des journaux.

```
# Get an AWS Identity and Access Management (IAM) role.
#
# @param iam_role_name: The name of the role to retrieve.
# @param action: Whether to create or destroy the IAM apparatus.
# @return: The IAM role.
def manage_iam(iam_role_name, action)
  case action
  when 'create'
    create_iam_role(iam_role_name)
  when 'destroy'
    destroy_iam_role(iam_role_name)
  else
    raise "Incorrect action provided. Must provide 'create' or 'destroy'"
  end
end

private

def create_iam_role(iam_role_name)
```

```
    role_policy = {
      'Version': '2012-10-17',
      'Statement': [
        {
          'Effect': 'Allow',
          'Principal': { 'Service': 'lambda.amazonaws.com' },
          'Action': 'sts:AssumeRole'
        }
      ]
    }
    role = @iam_client.create_role(
      role_name: iam_role_name,
      assume_role_policy_document: role_policy.to_json
    )
    @iam_client.attach_role_policy(
      {
        policy_arn: 'arn:aws:iam::aws:policy/service-role/
AWSLambdaBasicExecutionRole',
        role_name: iam_role_name
      }
    )
    wait_for_role_to_exist(iam_role_name)
    @logger.debug("Successfully created IAM role: #{role['role']['arn']}")
    sleep(10)
    [role, role_policy.to_json]
  end

  def destroy_iam_role(iam_role_name)
    @iam_client.detach_role_policy(
      {
        policy_arn: 'arn:aws:iam::aws:policy/service-role/
AWSLambdaBasicExecutionRole',
        role_name: iam_role_name
      }
    )
    @iam_client.delete_role(role_name: iam_role_name)
    @logger.debug("Detached policy & deleted IAM role: #{iam_role_name}")
  end

  def wait_for_role_to_exist(iam_role_name)
    @iam_client.wait_until(:role_exists, { role_name: iam_role_name }) do |w|
      w.max_attempts = 5
      w.delay = 5
    end
```

```
  end
```

Définissez un gestionnaire Lambda qui incrémente un nombre fourni en tant que paramètre d'invocation.

```
require 'logger'

# A function that increments a whole number by one (1) and logs the result.
# Requires a manually-provided runtime parameter, 'number', which must be Int
#
# @param event [Hash] Parameters sent when the function is invoked
# @param context [Hash] Methods and properties that provide information
# about the invocation, function, and execution environment.
# @return incremented_number [String] The incremented number.
def lambda_handler(event:, context:)
  logger = Logger.new($stdout)
  log_level = ENV['LOG_LEVEL']
  logger.level = case log_level
                 when 'debug'
                   Logger::DEBUG
                 when 'info'
                   Logger::INFO
                 else
                   Logger::ERROR
                 end
  logger.debug('This is a debug log message.')
  logger.info('This is an info log message. Code executed successfully!')
  number = event['number'].to_i
  incremented_number = number + 1
  logger.info("You provided #{number.round} and it was incremented to
 #{incremented_number.round}")
  incremented_number.round.to_s
end
```

Zippez votre fonction Lambda dans un package de déploiement.

```
  # Creates a Lambda deployment package in .zip format.
  #
  # @param source_file: The name of the object, without suffix, for the Lambda
 file and zip.
  # @return: The deployment package.
```

```
 def create_deployment_package(source_file)
   Dir.chdir(File.dirname(__FILE__))
   if File.exist?('lambda_function.zip')
     File.delete('lambda_function.zip')
     @logger.debug('Deleting old zip: lambda_function.zip')
   end
   Zip::File.open('lambda_function.zip', create: true) do |zipfile|
     zipfile.add('lambda_function.rb', "#{source_file}.rb")
   end
   @logger.debug("Zipping #{source_file}.rb into: lambda_function.zip.")
   File.read('lambda_function.zip').to_s
 rescue StandardError => e
   @logger.error("There was an error creating deployment package:\n
#{e.message}")
 end
```

Créez une fonction Lambda.

```
 # Deploys a Lambda function.
 #
 # @param function_name: The name of the Lambda function.
 # @param handler_name: The fully qualified name of the handler function.
 # @param role_arn: The IAM role to use for the function.
 # @param deployment_package: The deployment package that contains the function
code in .zip format.
 # @return: The Amazon Resource Name (ARN) of the newly created function.
 def create_function(function_name, handler_name, role_arn, deployment_package)
   response = @lambda_client.create_function({
                                               role: role_arn.to_s,
                                               function_name: function_name,
                                               handler: handler_name,
                                               runtime: 'ruby2.7',
                                               code: {
                                                 zip_file: deployment_package
                                               },
                                               environment: {
                                                 variables: {
                                                   'LOG_LEVEL' => 'info'
                                                 }
                                               }
                                             })
```

```
    @lambda_client.wait_until(:function_active_v2, { function_name:
function_name }) do |w|
      w.max_attempts = 5
      w.delay = 5
    end
    response
  rescue Aws::Lambda::Errors::ServiceException => e
    @logger.error("There was an error creating #{function_name}:\n #{e.message}")
  rescue Aws::Waiters::Errors::WaiterFailed => e
    @logger.error("Failed waiting for #{function_name} to activate:\n
#{e.message}")
  end
```

Invoquez votre fonction Lambda avec des paramètres d'exécution facultatifs.

```
  # Invokes a Lambda function.
  # @param function_name [String] The name of the function to invoke.
  # @param payload [nil] Payload containing runtime parameters.
  # @return [Object] The response from the function invocation.
  def invoke_function(function_name, payload = nil)
    params = { function_name: function_name }
    params[:payload] = payload unless payload.nil?
    @lambda_client.invoke(params)
  rescue Aws::Lambda::Errors::ServiceException => e
    @logger.error("There was an error executing #{function_name}:\n
#{e.message}")
  end
```

Mettez la configuration de votre fonction Lambda à jour pour injecter une nouvelle variable d'environnement.

```
  # Updates the environment variables for a Lambda function.
  # @param function_name: The name of the function to update.
  # @param log_level: The log level of the function.
  # @return: Data about the update, including the status.
  def update_function_configuration(function_name, log_level)
    @lambda_client.update_function_configuration({
                                                   function_name: function_name,
                                                   environment: {
                                                     variables: {
                                                       'LOG_LEVEL' => log_level
```

```
                                                    }
                                                  }
                                                })
    @lambda_client.wait_until(:function_updated_v2, { function_name:
function_name }) do |w|
      w.max_attempts = 5
      w.delay = 5
    end
  rescue Aws::Lambda::Errors::ServiceException => e
    @logger.error("There was an error updating configurations for
#{function_name}:\n #{e.message}")
  rescue Aws::Waiters::Errors::WaiterFailed => e
    @logger.error("Failed waiting for #{function_name} to activate:\n
#{e.message}")
  end
```

Mettez le code de votre fonction Lambda à jour avec un package de déploiement différent contenant un code différent.

```
  # Updates the code for a Lambda function by submitting a .zip archive that
contains
  # the code for the function.
  #
  # @param function_name: The name of the function to update.
  # @param deployment_package: The function code to update, packaged as bytes in
  #                            .zip format.
  # @return: Data about the update, including the status.
  def update_function_code(function_name, deployment_package)
    @lambda_client.update_function_code(
      function_name: function_name,
      zip_file: deployment_package
    )
    @lambda_client.wait_until(:function_updated_v2, { function_name:
function_name }) do |w|
      w.max_attempts = 5
      w.delay = 5
    end
  rescue Aws::Lambda::Errors::ServiceException => e
    @logger.error("There was an error updating function code for:
#{function_name}:\n #{e.message}")
    nil
  rescue Aws::Waiters::Errors::WaiterFailed => e
```

```
    @logger.error("Failed waiting for #{function_name} to update:\n
#{e.message}")
  end
```

Répertoriez toutes les fonctions Lambda existantes à l'aide du programme de pagination intégré.

```
# Lists the Lambda functions for the current account.
def list_functions
  functions = []
  @lambda_client.list_functions.each do |response|
    response['functions'].each do |function|
      functions.append(function['function_name'])
    end
  end
  functions
rescue Aws::Lambda::Errors::ServiceException => e
  @logger.error("There was an error listing functions:\n #{e.message}")
end
```

Supprimez une fonction Lambda spécifique.

```
# Deletes a Lambda function.
# @param function_name: The name of the function to delete.
def delete_function(function_name)
  print "Deleting function: #{function_name}..."
  @lambda_client.delete_function(
    function_name: function_name
  )
  print 'Done!'.green
rescue Aws::Lambda::Errors::ServiceException => e
  @logger.error("There was an error deleting #{function_name}:\n #{e.message}")
end
```

- Pour plus d'informations sur l'API, consultez les rubriques suivantes dans la référence de l'API AWS SDK pour Ruby .
  - CreateFunction
  - DeleteFunction

- GetFunction
- Invoke
- ListFunctions
- UpdateFunctionCode
- UpdateFunctionConfiguration

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Le Cargo.toml avec des dépendances utilisées dans ce scénario.

```
[package]
name = "lambda-code-examples"
version = "0.1.0"
edition = "2021"

# See more keys and their definitions at https://doc.rust-lang.org/cargo/
reference/manifest.html

[dependencies]
aws-config = { version = "1.0.1", features = ["behavior-version-latest"] }
aws-sdk-ec2 = { version = "1.3.0" }
aws-sdk-iam = { version = "1.3.0" }
aws-sdk-lambda = { version = "1.3.0" }
aws-sdk-s3 = { version = "1.4.0" }
aws-smithy-types = { version = "1.0.1" }
aws-types = { version = "1.0.1" }
clap = { version = "4.4", features = ["derive"] }
tokio = { version = "1.20.1", features = ["full"] }
tracing-subscriber = { version = "0.3.15", features = ["env-filter"] }
tracing = "0.1.37"
serde_json = "1.0.94"
anyhow = "1.0.71"
```

```
uuid = { version = "1.3.3", features = ["v4"] }
lambda_runtime = "0.8.0"
serde = "1.0.164"
```

Un ensemble d'utilitaires qui simplifient l'appel à Lambda pour ce scénario. Ce fichier est src/ations.rs dans la caisse.

```
use anyhow::anyhow;
use aws_sdk_iam::operation::{create_role::CreateRoleError,
 delete_role::DeleteRoleOutput};
use aws_sdk_lambda::{
    operation::{
        delete_function::DeleteFunctionOutput, get_function::GetFunctionOutput,
        invoke::InvokeOutput, list_functions::ListFunctionsOutput,
        update_function_code::UpdateFunctionCodeOutput,
        update_function_configuration::UpdateFunctionConfigurationOutput,
    },
    primitives::ByteStream,
    types::{Environment, FunctionCode, LastUpdateStatus, State},
};
use aws_sdk_s3::{
    error::ErrorMetadata,
    operation::{delete_bucket::DeleteBucketOutput,
 delete_object::DeleteObjectOutput},
    types::CreateBucketConfiguration,
};
use aws_smithy_types::Blob;
use serde::{ser::SerializeMap, Serialize};
use std::{fmt::Display, path::PathBuf, str::FromStr, time::Duration};
use tracing::{debug, info, warn};

/* Operation describes  */
#[derive(Clone, Copy, Debug, Serialize)]
pub enum Operation {
    #[serde(rename = "plus")]
    Plus,
    #[serde(rename = "minus")]
    Minus,
    #[serde(rename = "times")]
    Times,
    #[serde(rename = "divided-by")]
```

```
    DividedBy,
}

impl FromStr for Operation {
    type Err = anyhow::Error;

    fn from_str(s: &str) -> Result<Self, Self::Err> {
        match s {
            "plus" => Ok(Operation::Plus),
            "minus" => Ok(Operation::Minus),
            "times" => Ok(Operation::Times),
            "divided-by" => Ok(Operation::DividedBy),
            _ => Err(anyhow!("Unknown operation {s}")),
        }
    }
}

impl Display for Operation {
    fn fmt(&self, f: &mut std::fmt::Formatter<'_>) -> std::fmt::Result {
        match self {
            Operation::Plus => write!(f, "plus"),
            Operation::Minus => write!(f, "minus"),
            Operation::Times => write!(f, "times"),
            Operation::DividedBy => write!(f, "divided-by"),
        }
    }
}

/**
 * InvokeArgs will be serialized as JSON and sent to the AWS Lambda handler.
 */
#[derive(Debug)]
pub enum InvokeArgs {
    Increment(i32),
    Arithmetic(Operation, i32, i32),
}

impl Serialize for InvokeArgs {
    fn serialize<S>(&self, serializer: S) -> Result<S::Ok, S::Error>
    where
        S: serde::Serializer,
    {
        match self {
            InvokeArgs::Increment(i) => serializer.serialize_i32(*i),
```

```
            InvokeArgs::Arithmetic(o, i, j) => {
                let mut map: S::SerializeMap =
 serializer.serialize_map(Some(3))?;
                map.serialize_key(&"op".to_string())?;
                map.serialize_value(&o.to_string())?;
                map.serialize_key(&"i".to_string())?;
                map.serialize_value(&i)?;
                map.serialize_key(&"j".to_string())?;
                map.serialize_value(&j)?;
                map.end()
            }
        }
    }
}

/** A policy document allowing Lambda to execute this function on the account's
 behalf. */
const ROLE_POLICY_DOCUMENT: &str = r#"{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": { "Service": "lambda.amazonaws.com" },
            "Action": "sts:AssumeRole"
        }
    ]
}"#;

/**
 * A LambdaManager gathers all the resources necessary to run the Lambda example
 scenario.
 * This includes instantiated aws_sdk clients and details of resource names.
 */
pub struct LambdaManager {
    iam_client: aws_sdk_iam::Client,
    lambda_client: aws_sdk_lambda::Client,
    s3_client: aws_sdk_s3::Client,
    lambda_name: String,
    role_name: String,
    bucket: String,
    own_bucket: bool,
}
```

```
// These unit type structs provide nominal typing on top of String parameters for
 LambdaManager::new
pub struct LambdaName(pub String);
pub struct RoleName(pub String);
pub struct Bucket(pub String);
pub struct OwnBucket(pub bool);

impl LambdaManager {
    pub fn new(
        iam_client: aws_sdk_iam::Client,
        lambda_client: aws_sdk_lambda::Client,
        s3_client: aws_sdk_s3::Client,
        lambda_name: LambdaName,
        role_name: RoleName,
        bucket: Bucket,
        own_bucket: OwnBucket,
    ) -> Self {
        Self {
            iam_client,
            lambda_client,
            s3_client,
            lambda_name: lambda_name.0,
            role_name: role_name.0,
            bucket: bucket.0,
            own_bucket: own_bucket.0,
        }
    }

    /**
     * Load the AWS configuration from the environment.
     * Look up lambda_name and bucket if none are given, or generate a random
 name if not present in the environment.
     * If the bucket name is provided, the caller needs to have created the
 bucket.
     * If the bucket name is generated, it will be created.
     */
    pub async fn load_from_env(lambda_name: Option<String>, bucket:
 Option<String>) -> Self {
        let sdk_config = aws_config::load_from_env().await;
        let lambda_name = LambdaName(lambda_name.unwrap_or_else(|| {
            std::env::var("LAMBDA_NAME").unwrap_or_else(|_|
 "rust_lambda_example".to_string())
        }));
        let role_name = RoleName(format!("{}_role", lambda_name.0));
```

```
        let (bucket, own_bucket) =
            match bucket {
                Some(bucket) => (Bucket(bucket), false),
                None => (
                    Bucket(std::env::var("LAMBDA_BUCKET").unwrap_or_else(|_| {
                        format!("rust-lambda-example-{}", uuid::Uuid::new_v4())
                    })),
                    true,
                ),
            };

        let s3_client = aws_sdk_s3::Client::new(&sdk_config);

        if own_bucket {
            info!("Creating bucket for demo: {}", bucket.0);
            s3_client
                .create_bucket()
                .bucket(bucket.0.clone())
                .create_bucket_configuration(
                    CreateBucketConfiguration::builder()

.location_constraint(aws_sdk_s3::types::BucketLocationConstraint::from(
                            sdk_config.region().unwrap().as_ref(),
                        ))
                        .build(),
                )
                .send()
                .await
                .unwrap();
        }

        Self::new(
            aws_sdk_iam::Client::new(&sdk_config),
            aws_sdk_lambda::Client::new(&sdk_config),
            s3_client,
            lambda_name,
            role_name,
            bucket,
            OwnBucket(own_bucket),
        )
    }

    /**
     * Upload function code from a path to a zip file.
```

```
     * The zip file must have an AL2 Linux-compatible binary called `bootstrap`.
     * The easiest way to create such a zip is to use `cargo lambda build --
output-format Zip`.
     */
    async fn prepare_function(
        &self,
        zip_file: PathBuf,
        key: Option<String>,
    ) -> Result<FunctionCode, anyhow::Error> {
        let body = ByteStream::from_path(zip_file).await?;

        let key = key.unwrap_or_else(|| format!("{}_code", self.lambda_name));

        info!("Uploading function code to s3://{}/{}", self.bucket, key);
        let _ = self
            .s3_client
            .put_object()
            .bucket(self.bucket.clone())
            .key(key.clone())
            .body(body)
            .send()
            .await?;

        Ok(FunctionCode::builder()
            .s3_bucket(self.bucket.clone())
            .s3_key(key)
            .build())
    }

    /**
     * Create a function, uploading from a zip file.
     */
    pub async fn create_function(&self, zip_file: PathBuf) -> Result<String,
 anyhow::Error> {
        let code = self.prepare_function(zip_file, None).await?;

        let key = code.s3_key().unwrap().to_string();

        let role = self.create_role().await.map_err(|e| anyhow!(e))?;

        info!("Created iam role, waiting 15s for it to become active");
        tokio::time::sleep(Duration::from_secs(15)).await;

        info!("Creating lambda function {}", self.lambda_name);
```

```
        let _ = self
            .lambda_client
            .create_function()
            .function_name(self.lambda_name.clone())
            .code(code)
            .role(role.arn())
            .runtime(aws_sdk_lambda::types::Runtime::Providedal2)
            .handler("_unused")
            .send()
            .await
            .map_err(anyhow::Error::from)?;

        self.wait_for_function_ready().await?;

        self.lambda_client
            .publish_version()
            .function_name(self.lambda_name.clone())
            .send()
            .await?;

        Ok(key)
    }

    /**
     * Create an IAM execution role for the managed Lambda function.
     * If the role already exists, use that instead.
     */
    async fn create_role(&self) -> Result<aws_sdk_iam::types::Role,
CreateRoleError> {
        info!("Creating execution role for function");
        let get_role = self
            .iam_client
            .get_role()
            .role_name(self.role_name.clone())
            .send()
            .await;
        if let Ok(get_role) = get_role {
            if let Some(role) = get_role.role {
                return Ok(role);
            }
        }

        let create_role = self
            .iam_client
```

```
            .create_role()
            .role_name(self.role_name.clone())
            .assume_role_policy_document(ROLE_POLICY_DOCUMENT)
            .send()
            .await;

        match create_role {
            Ok(create_role) => match create_role.role {
                Some(role) => Ok(role),
                None => Err(CreateRoleError::generic(
                    ErrorMetadata::builder()
                        .message("CreateRole returned empty success")
                        .build(),
                )),
            },
            Err(err) => Err(err.into_service_error()),
        }
    }

    /**
     * Poll `is_function_ready` with a 1-second delay. It returns when the
function is ready or when there's an error checking the function's state.
     */
    pub async fn wait_for_function_ready(&self) -> Result<(), anyhow::Error> {
        info!("Waiting for function");
        while !self.is_function_ready(None).await? {
            info!("Function is not ready, sleeping 1s");
            tokio::time::sleep(Duration::from_secs(1)).await;
        }
        Ok(())
    }

    /**
     * Check if a Lambda function is ready to be invoked.
     * A Lambda function is ready for this scenario when its state is active and
its LastUpdateStatus is Successful.
     * Additionally, if a sha256 is provided, the function must have that as its
current code hash.
     * Any missing properties or failed requests will be reported as an Err.
     */
    async fn is_function_ready(
        &self,
        expected_code_sha256: Option<&str>,
    ) -> Result<bool, anyhow::Error> {
```

```
        match self.get_function().await {
            Ok(func) => {
                if let Some(config) = func.configuration() {
                    if let Some(state) = config.state() {
                        info!(?state, "Checking if function is active");
                        if !matches!(state, State::Active) {
                            return Ok(false);
                        }
                    }
                    match config.last_update_status() {
                        Some(last_update_status) => {
                            info!(?last_update_status, "Checking if function is
ready");
                            match last_update_status {
                                LastUpdateStatus::Successful => {
                                    // continue
                                }
                                LastUpdateStatus::Failed |
LastUpdateStatus::InProgress => {
                                    return Ok(false);
                                }
                                unknown => {
                                    warn!(
                                        status_variant = unknown.as_str(),
                                        "LastUpdateStatus unknown"
                                    );
                                    return Err(anyhow!(
                                        "Unknown LastUpdateStatus, fn config is
{config:?}"
                                    ));
                                }
                            }
                        }
                        None => {
                            warn!("Missing last update status");
                            return Ok(false);
                        }
                    };
                    if expected_code_sha256.is_none() {
                        return Ok(true);
                    }
                    if let Some(code_sha256) = config.code_sha256() {
                        return Ok(code_sha256 ==
expected_code_sha256.unwrap_or_default());
```

```
                    }
                }
            }
            Err(e) => {
                warn!(?e, "Could not get function while waiting");
            }
        }
        Ok(false)
    }

    /** Get the Lambda function with this Manager's name. */
    pub async fn get_function(&self) -> Result<GetFunctionOutput, anyhow::Error>
{
        info!("Getting lambda function");
        self.lambda_client
            .get_function()
            .function_name(self.lambda_name.clone())
            .send()
            .await
            .map_err(anyhow::Error::from)
    }

    /** List all Lambda functions in the current Region. */
    pub async fn list_functions(&self) -> Result<ListFunctionsOutput,
anyhow::Error> {
        info!("Listing lambda functions");
        self.lambda_client
            .list_functions()
            .send()
            .await
            .map_err(anyhow::Error::from)
    }

    /** Invoke the lambda function using calculator InvokeArgs. */
    pub async fn invoke(&self, args: InvokeArgs) -> Result<InvokeOutput,
anyhow::Error> {
        info!(?args, "Invoking {}", self.lambda_name);
        let payload = serde_json::to_string(&args)?;
        debug!(?payload, "Sending payload");
        self.lambda_client
            .invoke()
            .function_name(self.lambda_name.clone())
            .payload(Blob::new(payload))
            .send()
```

```
            .await
            .map_err(anyhow::Error::from)
    }

    /** Given a Path to a zip file, update the function's code and wait for the
update to finish. */
    pub async fn update_function_code(
        &self,
        zip_file: PathBuf,
        key: String,
    ) -> Result<UpdateFunctionCodeOutput, anyhow::Error> {
        let function_code = self.prepare_function(zip_file, Some(key)).await?;

        info!("Updating code for {}", self.lambda_name);
        let update = self
            .lambda_client
            .update_function_code()
            .function_name(self.lambda_name.clone())
            .s3_bucket(self.bucket.clone())
            .s3_key(function_code.s3_key().unwrap().to_string())
            .send()
            .await
            .map_err(anyhow::Error::from)?;

        self.wait_for_function_ready().await?;

        Ok(update)
    }

    /** Update the environment for a function. */
    pub async fn update_function_configuration(
        &self,
        environment: Environment,
    ) -> Result<UpdateFunctionConfigurationOutput, anyhow::Error> {
        info!(
            ?environment,
            "Updating environment for {}", self.lambda_name
        );
        let updated = self
            .lambda_client
            .update_function_configuration()
            .function_name(self.lambda_name.clone())
            .environment(environment)
            .send()
```

```
            .await
            .map_err(anyhow::Error::from)?;

        self.wait_for_function_ready().await?;

        Ok(updated)
    }

    /** Delete a function and its role, and if possible or necessary, its
associated code object and bucket. */
    pub async fn delete_function(
        &self,
        location: Option<String>,
    ) -> (
        Result<DeleteFunctionOutput, anyhow::Error>,
        Result<DeleteRoleOutput, anyhow::Error>,
        Option<Result<DeleteObjectOutput, anyhow::Error>>,
    ) {
        info!("Deleting lambda function {}", self.lambda_name);
        let delete_function = self
            .lambda_client
            .delete_function()
            .function_name(self.lambda_name.clone())
            .send()
            .await
            .map_err(anyhow::Error::from);

        info!("Deleting iam role {}", self.role_name);
        let delete_role = self
            .iam_client
            .delete_role()
            .role_name(self.role_name.clone())
            .send()
            .await
            .map_err(anyhow::Error::from);

        let delete_object: Option<Result<DeleteObjectOutput, anyhow::Error>> =
            if let Some(location) = location {
                info!("Deleting object {location}");
                Some(
                    self.s3_client
                        .delete_object()
                        .bucket(self.bucket.clone())
                        .key(location)
```

```
                        .send()
                        .await
                        .map_err(anyhow::Error::from),
                )
            } else {
                info!(?location, "Skipping delete object");
                None
            };

        (delete_function, delete_role, delete_object)
    }

    pub async fn cleanup(
        &self,
        location: Option<String>,
    ) -> (
        (
            Result<DeleteFunctionOutput, anyhow::Error>,
            Result<DeleteRoleOutput, anyhow::Error>,
            Option<Result<DeleteObjectOutput, anyhow::Error>>,
        ),
        Option<Result<DeleteBucketOutput, anyhow::Error>>,
    ) {
        let delete_function = self.delete_function(location).await;

        let delete_bucket = if self.own_bucket {
            info!("Deleting bucket {}", self.bucket);
            if delete_function.2.is_none() ||
delete_function.2.as_ref().unwrap().is_ok() {
                Some(
                    self.s3_client
                        .delete_bucket()
                        .bucket(self.bucket.clone())
                        .send()
                        .await
                        .map_err(anyhow::Error::from),
                )
            } else {
                None
            }
        } else {
            info!("No bucket to clean up");
            None
        };
```

```
        (delete_function, delete_bucket)
    }
}

/**
 * Testing occurs primarily as an integration test running the `scenario` bin
 successfully.
 * Each action relies deeply on the internal workings and state of Amazon Simple
 Storage Service (Amazon S3), Lambda, and IAM working together.
 * It is therefore infeasible to mock the clients to test the individual actions.
 */
#[cfg(test)]
mod test {
    use super::{InvokeArgs, Operation};
    use serde_json::json;

    /** Make sure that the JSON output of serializing InvokeArgs is what's
 expected by the calculator. */
    #[test]
    fn test_serialize() {
        assert_eq!(json!(InvokeArgs::Increment(5)), 5);
        assert_eq!(
            json!(InvokeArgs::Arithmetic(Operation::Plus, 5, 7)).to_string(),
            r#"{"op":"plus","i":5,"j":7}"#.to_string(),
        );
    }
}
```

Un binaire pour exécuter le scénario de bout en bout, en utilisant des indicateurs de ligne de commande pour contrôler certains comportements. Ce fichier est src/bin/scenario.rs dans la caisse.

```
/*
## Service actions

Service actions wrap the SDK call, taking a client and any specific parameters
 necessary for the call.

* CreateFunction
* GetFunction
```

```
* ListFunctions
* Invoke
* UpdateFunctionCode
* UpdateFunctionConfiguration
* DeleteFunction

## Scenario
A scenario runs at a command prompt and prints output to the user on the result
 of each service action. A scenario can run in one of two ways: straight through,
 printing out progress as it goes, or as an interactive question/answer script.

## Getting started with functions

Use an SDK to manage AWS Lambda functions: create a function, invoke it, update
 its code, invoke it again, view its output and logs, and delete it.

This scenario uses two Lambda handlers:
_Note: Handlers don't use AWS SDK API calls._

The increment handler is straightforward:

1. It accepts a number, increments it, and returns the new value.
2. It performs simple logging of the result.

The arithmetic handler is more complex:
1. It accepts a set of actions ['plus', 'minus', 'times', 'divided-by'] and two
 numbers, and returns the result of the calculation.
2. It uses an environment variable to control log level (such as DEBUG, INFO,
 WARNING, ERROR).
It logs a few things at different levels, such as:
    * DEBUG: Full event data.
    * INFO: The calculation result.
    * WARN~ING~: When a divide by zero error occurs.
    * This will be the typical `RUST_LOG` variable.


The steps of the scenario are:

1. Create an AWS Identity and Access Management (IAM) role that meets the
 following requirements:
    * Has an assume_role policy that grants 'lambda.amazonaws.com' the
 'sts:AssumeRole' action.
    * Attaches the 'arn:aws:iam::aws:policy/service-role/
AWSLambdaBasicExecutionRole' managed role.
```

```
    * _You must wait for ~10 seconds after the role is created before you can use
 it!_
2. Create a function (CreateFunction) for the increment handler by packaging it
 as a zip and doing one of the following:
    * Adding it with CreateFunction Code.ZipFile.
    * --or--
    * Uploading it to Amazon Simple Storage Service (Amazon S3) and adding it
 with CreateFunction Code.S3Bucket/S3Key.
    * _Note: Zipping the file does not have to be done in code._
    * If you have a waiter, use it to wait until the function is active.
 Otherwise, call GetFunction until State is Active.
3. Invoke the function with a number and print the result.
4. Update the function (UpdateFunctionCode) to the arithmetic handler by
 packaging it as a zip and doing one of the following:
    * Adding it with UpdateFunctionCode ZipFile.
    * --or--
    * Uploading it to Amazon S3 and adding it with UpdateFunctionCode S3Bucket/
S3Key.
5. Call GetFunction until Configuration.LastUpdateStatus is 'Successful' (or
 'Failed').
6. Update the environment variable by calling UpdateFunctionConfiguration and
 pass it a log level, such as:
    * Environment={'Variables': {'RUST_LOG': 'TRACE'}}
7. Invoke the function with an action from the list and a couple of values.
 Include LogType='Tail' to get logs in the result. Print the result of the
 calculation and the log.
8. [Optional] Invoke the function to provoke a divide-by-zero error and show the
 log result.
9. List all functions for the account, using pagination (ListFunctions).
10. Delete the function (DeleteFunction).
11. Delete the role.

Each step should use the function created in Service Actions to abstract calling
 the SDK.
 */

use aws_sdk_lambda::{operation::invoke::InvokeOutput, types::Environment};
use clap::Parser;
use std::{collections::HashMap, path::PathBuf};
use tracing::{debug, info, warn};
use tracing_subscriber::EnvFilter;

use lambda_code_examples::actions::{
    InvokeArgs::{Arithmetic, Increment},
```

```
    LambdaManager, Operation,
};

#[derive(Debug, Parser)]
pub struct Opt {
    /// The AWS Region.
    #[structopt(short, long)]
    pub region: Option<String>,

    // The bucket to use for the FunctionCode.
    #[structopt(short, long)]
    pub bucket: Option<String>,

    // The name of the Lambda function.
    #[structopt(short, long)]
    pub lambda_name: Option<String>,

    // The number to increment.
    #[structopt(short, long, default_value = "12")]
    pub inc: i32,

    // The left operand.
    #[structopt(long, default_value = "19")]
    pub num_a: i32,

    // The right operand.
    #[structopt(long, default_value = "23")]
    pub num_b: i32,

    // The arithmetic operation.
    #[structopt(short, long, default_value = "plus")]
    pub operation: Operation,

    #[structopt(long)]
    pub cleanup: Option<bool>,

    #[structopt(long)]
    pub no_cleanup: Option<bool>,
}

fn code_path(lambda: &str) -> PathBuf {
    PathBuf::from(format!("../target/lambda/{lambda}/bootstrap.zip"))
}
```

```
fn log_invoke_output(invoke: &InvokeOutput, message: &str) {
    if let Some(payload) = invoke.payload().cloned() {
        let payload = String::from_utf8(payload.into_inner());
        info!(?payload, message);
    } else {
        info!("Could not extract payload")
    }
    if let Some(logs) = invoke.log_result() {
        debug!(?logs, "Invoked function logs")
    } else {
        debug!("Invoked function had no logs")
    }
}

async fn main_block(
    opt: &Opt,
    manager: &LambdaManager,
    code_location: String,
) -> Result<(), anyhow::Error> {
    let invoke = manager.invoke(Increment(opt.inc)).await?;
    log_invoke_output(&invoke, "Invoked function configured as increment");

    let update_code = manager
        .update_function_code(code_path("arithmetic"), code_location.clone())
        .await?;

    let code_sha256 = update_code.code_sha256().unwrap_or("Unknown SHA");
    info!(?code_sha256, "Updated function code with arithmetic.zip");

    let arithmetic_args = Arithmetic(opt.operation, opt.num_a, opt.num_b);
    let invoke = manager.invoke(arithmetic_args).await?;
    log_invoke_output(&invoke, "Invoked function configured as arithmetic");

    let update = manager
        .update_function_configuration(
            Environment::builder()
                .set_variables(Some(HashMap::from([(
                    "RUST_LOG".to_string(),
                    "trace".to_string(),
                )])))
                .build(),
        )
        .await?;
    let updated_environment = update.environment();
```

```
    info!(?updated_environment, "Updated function configuration");

    let invoke = manager
        .invoke(Arithmetic(opt.operation, opt.num_a, opt.num_b))
        .await?;
    log_invoke_output(
        &invoke,
        "Invoked function configured as arithmetic with increased logging",
    );

    let invoke = manager
        .invoke(Arithmetic(Operation::DividedBy, opt.num_a, 0))
        .await?;
    log_invoke_output(
        &invoke,
        "Invoked function configured as arithmetic with divide by zero",
    );

    Ok::<(), anyhow::Error>(())
}

#[tokio::main]
async fn main() {
    tracing_subscriber::fmt()
        .without_time()
        .with_file(true)
        .with_line_number(true)
        .with_env_filter(EnvFilter::from_default_env())
        .init();

    let opt = Opt::parse();
    let manager = LambdaManager::load_from_env(opt.lambda_name.clone(),
 opt.bucket.clone()).await;

    let key = match manager.create_function(code_path("increment")).await {
        Ok(init) => {
            info!(?init, "Created function, initially with increment.zip");
            let run_block = main_block(&opt, &manager, init.clone()).await;
            info!(?run_block, "Finished running example, cleaning up");
            Some(init)
        }
        Err(err) => {
            warn!(?err, "Error happened when initializing function");
            None
```

```
        }
    };

    if Some(false) == opt.cleanup || Some(true) == opt.no_cleanup {
        info!("Skipping cleanup")
    } else {
        let delete = manager.cleanup(key).await;
        info!(?delete, "Deleted function & cleaned up resources");
    }
}
```

- Pour plus de détails sur l'API, consultez les rubriques suivantes dans la Référence des API du kit AWS SDK pour Rust.
  - CreateFunction
  - DeleteFunction
  - GetFunction
  - Invoke
  - ListFunctions
  - UpdateFunctionCode
  - UpdateFunctionConfiguration

SAP ABAP

Kit SDK pour SAP ABAP

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
   TRY.
       "Create an AWS Identity and Access Management (IAM) role that grants AWS
Lambda permission to write to logs."
       DATA(lv_policy_document) = `{` &&
           `"Version":"2012-10-17",       ` &&
```

```
                  `"Statement": [` &&
                    `{` &&
                      `"Effect": "Allow",` &&
                      `"Action": [` &&
                        `"sts:AssumeRole"` &&
                      `],` &&
                      `"Principal": {` &&
                        `"Service": [` &&
                          `"lambda.amazonaws.com"` &&
                        `]` &&
                      `}` &&
                    `}` &&
                  `]` &&
                `}`.
        TRY.
            DATA(lo_create_role_output) = lo_iam->createrole(
                    iv_rolename = iv_role_name
                    iv_assumerolepolicydocument = lv_policy_document
                    iv_description = 'Grant lambda permission to write to
 logs' ).
            DATA(lv_role_arn) = lo_create_role_output->get_role( )->get_arn( ).
            MESSAGE 'IAM role created.' TYPE 'I'.
            WAIT UP TO 10 SECONDS.            " Make sure that the IAM role is
 ready for use. "
          CATCH /aws1/cx_iamentityalrdyexex.
            DATA(lo_role) = lo_iam->getrole( iv_rolename = iv_role_name ).
            lv_role_arn = lo_role->get_role( )->get_arn( ).
          CATCH /aws1/cx_iaminvalidinputex.
            MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
          CATCH /aws1/cx_iammalformedplydocex.
            MESSAGE 'Policy document in the request is malformed.' TYPE 'E'.
        ENDTRY.

        TRY.
            lo_iam->attachrolepolicy(
                iv_rolename  = iv_role_name
                iv_policyarn = 'arn:aws:iam::aws:policy/service-role/
AWSLambdaBasicExecutionRole' ).
            MESSAGE 'Attached policy to the IAM role.' TYPE 'I'.
          CATCH /aws1/cx_iaminvalidinputex.
            MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
          CATCH /aws1/cx_iamnosuchentityex.
            MESSAGE 'The requested resource entity does not exist.' TYPE 'E'.
          CATCH /aws1/cx_iamplynotattachableex.
```

```
            MESSAGE 'Service role policies can only be attached to the service-
linked role for their service.' TYPE 'E'.
          CATCH /aws1/cx_iamunmodableentityex.
            MESSAGE 'Service that depends on the service-linked role is not
 modifiable.' TYPE 'E'.
        ENDTRY.

        " Create a Lambda function and upload handler code. "
        " Lambda function performs 'increment' action on a number. "
        TRY.
            lo_lmd->createfunction(
                 iv_functionname = iv_function_name
                 iv_runtime = `python3.9`
                 iv_role = lv_role_arn
                 iv_handler = iv_handler
                 io_code = io_initial_zip_file
                 iv_description = 'AWS Lambda code example' ).
            MESSAGE 'Lambda function created.' TYPE 'I'.
          CATCH /aws1/cx_lmdcodestorageexcdex.
            MESSAGE 'Maximum total code size per account exceeded.' TYPE 'E'.
          CATCH /aws1/cx_lmdinvparamvalueex.
            MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
          CATCH /aws1/cx_lmdresourcenotfoundex.
            MESSAGE 'The requested resource does not exist.' TYPE 'E'.
        ENDTRY.

        " Verify the function is in Active state "
        WHILE lo_lmd->getfunction( iv_functionname = iv_function_name )-
>get_configuration( )->ask_state( ) <> 'Active'.
          IF sy-index = 10.
            EXIT.               " Maximum 10 seconds. "
          ENDIF.
          WAIT UP TO 1 SECONDS.
        ENDWHILE.

        "Invoke the function with a single parameter and get results."
        TRY.
            DATA(lv_json) = /aws1/cl_rt_util=>string_to_xstring(
              `{`  &&
                `"action": "increment",`  &&
                `"number": 10` &&
              `}` ).
            DATA(lo_initial_invoke_output) = lo_lmd->invoke(
                       iv_functionname = iv_function_name
```

```
                        iv_payload = lv_json ).
            ov_initial_invoke_payload = lo_initial_invoke_output->get_payload( ).
           " ov_initial_invoke_payload is returned for testing purposes. "
            DATA(lo_writer_json) = cl_sxml_string_writer=>create( type =
 if_sxml=>co_xt_json ).
            CALL TRANSFORMATION id SOURCE XML ov_initial_invoke_payload RESULT
 XML lo_writer_json.
            DATA(lv_result) = cl_abap_codepage=>convert_from( lo_writer_json-
>get_output( ) ).
            MESSAGE 'Lambda function invoked.' TYPE 'I'.
          CATCH /aws1/cx_lmdinvparamvalueex.
            MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
          CATCH /aws1/cx_lmdinvrequestcontex.
            MESSAGE 'Unable to parse request body as JSON.' TYPE 'E'.
          CATCH /aws1/cx_lmdresourcenotfoundex.
            MESSAGE 'The requested resource does not exist.' TYPE 'E'.
          CATCH /aws1/cx_lmdunsuppedmediatyp00.
            MESSAGE 'Invoke request body does not have JSON as its content type.'
 TYPE 'E'.
        ENDTRY.

        " Update the function code and configure its Lambda environment with an
 environment variable. "
        " Lambda function is updated to perform 'decrement' action also. "
        TRY.
            lo_lmd->updatefunctioncode(
                  iv_functionname = iv_function_name
                  iv_zipfile = io_updated_zip_file ).
            WAIT UP TO 10 SECONDS.            " Make sure that the update is
 completed. "
            MESSAGE 'Lambda function code updated.' TYPE 'I'.
          CATCH /aws1/cx_lmdcodestorageexcdex.
            MESSAGE 'Maximum total code size per account exceeded.' TYPE 'E'.
          CATCH /aws1/cx_lmdinvparamvalueex.
            MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
          CATCH /aws1/cx_lmdresourcenotfoundex.
            MESSAGE 'The requested resource does not exist.' TYPE 'E'.
        ENDTRY.

        TRY.
            DATA lt_variables TYPE /aws1/
cl_lmdenvironmentvaria00=>tt_environmentvariables.
            DATA ls_variable LIKE LINE OF lt_variables.
            ls_variable-key = 'LOG_LEVEL'.
```

```
            ls_variable-value = NEW /aws1/cl_lmdenvironmentvaria00( iv_value =
 'info' ).
            INSERT ls_variable INTO TABLE lt_variables.

            lo_lmd->updatefunctionconfiguration(
                  iv_functionname = iv_function_name
                  io_environment = NEW /aws1/cl_lmdenvironment( it_variables =
 lt_variables ) ).
            WAIT UP TO 10 SECONDS.            " Make sure that the update is
 completed. "
            MESSAGE 'Lambda function configuration/settings updated.' TYPE 'I'.
          CATCH /aws1/cx_lmdinvparamvalueex.
            MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
          CATCH /aws1/cx_lmdresourceconflictex.
            MESSAGE 'Resource already exists or another operation is in
 progress.' TYPE 'E'.
          CATCH /aws1/cx_lmdresourcenotfoundex.
            MESSAGE 'The requested resource does not exist.' TYPE 'E'.
        ENDTRY.

        "Invoke the function with new parameters and get results. Display the
 execution log that's returned from the invocation."
        TRY.
            lv_json = /aws1/cl_rt_util=>string_to_xstring(
              `{`  &&
                `"action": "decrement",`  &&
                `"number": 10` &&
              `}` ).
            DATA(lo_updated_invoke_output) = lo_lmd->invoke(
                       iv_functionname = iv_function_name
                       iv_payload = lv_json ).
            ov_updated_invoke_payload = lo_updated_invoke_output->get_payload( ).
           " ov_updated_invoke_payload is returned for testing purposes. "
            lo_writer_json = cl_sxml_string_writer=>create( type =
 if_sxml=>co_xt_json ).
            CALL TRANSFORMATION id SOURCE XML ov_updated_invoke_payload RESULT
 XML lo_writer_json.
            lv_result = cl_abap_codepage=>convert_from( lo_writer_json-
>get_output( ) ).
            MESSAGE 'Lambda function invoked.' TYPE 'I'.
          CATCH /aws1/cx_lmdinvparamvalueex.
            MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
          CATCH /aws1/cx_lmdinvrequestcontex.
            MESSAGE 'Unable to parse request body as JSON.' TYPE 'E'.
```

```
          CATCH /aws1/cx_lmdresourcenotfoundex.
            MESSAGE 'The requested resource does not exist.' TYPE 'E'.
          CATCH /aws1/cx_lmdunsuppedmediatyp00.
            MESSAGE 'Invoke request body does not have JSON as its content type.'
 TYPE 'E'.
        ENDTRY.

        " List the functions for your account. "
        TRY.
            DATA(lo_list_output) = lo_lmd->listfunctions( ).
            DATA(lt_functions) = lo_list_output->get_functions( ).
            MESSAGE 'Retrieved list of Lambda functions.' TYPE 'I'.
          CATCH /aws1/cx_lmdinvparamvalueex.
            MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
        ENDTRY.

        " Delete the Lambda function. "
        TRY.
            lo_lmd->deletefunction( iv_functionname = iv_function_name ).
            MESSAGE 'Lambda function deleted.' TYPE 'I'.
          CATCH /aws1/cx_lmdinvparamvalueex.
            MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
          CATCH /aws1/cx_lmdresourcenotfoundex.
            MESSAGE 'The requested resource does not exist.' TYPE 'W'.
        ENDTRY.

        " Detach role policy. "
        TRY.
            lo_iam->detachrolepolicy(
                iv_rolename  = iv_role_name
                iv_policyarn = 'arn:aws:iam::aws:policy/service-role/
AWSLambdaBasicExecutionRole' ).
            MESSAGE 'Detached policy from the IAM role.' TYPE 'I'.
          CATCH /aws1/cx_iaminvalidinputex.
            MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
          CATCH /aws1/cx_iamnosuchentityex.
            MESSAGE 'The requested resource entity does not exist.' TYPE 'W'.
          CATCH /aws1/cx_iamplynotattachableex.
            MESSAGE 'Service role policies can only be attached to the service-
linked role for their service.' TYPE 'E'.
          CATCH /aws1/cx_iamunmodableentityex.
            MESSAGE 'Service that depends on the service-linked role is not
 modifiable.' TYPE 'E'.
        ENDTRY.
```

```
        " Delete the IAM role. "
        TRY.
            lo_iam->deleterole( iv_rolename = iv_role_name ).
            MESSAGE 'IAM role deleted.' TYPE 'I'.
          CATCH /aws1/cx_iamnosuchentityex.
            MESSAGE 'The requested resource entity does not exist.' TYPE 'W'.
          CATCH /aws1/cx_iamunmodableentityex.
            MESSAGE 'Service that depends on the service-linked role is not
modifiable.' TYPE 'E'.
        ENDTRY.

      CATCH /aws1/cx_rt_service_generic INTO lo_exception.
        DATA(lv_error) = lo_exception->get_longtext( ).
        MESSAGE lv_error TYPE 'E'.
    ENDTRY.
```

- Pour plus de détails sur l'API, consultez les rubriques suivantes dans la Référence des API du kit AWS SDK pour SAP ABAP.
  - CreateFunction
  - DeleteFunction
  - GetFunction
  - Invoke
  - ListFunctions
  - UpdateFunctionCode
  - UpdateFunctionConfiguration

Swift

Kit SDK pour Swift

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Définissez la première fonction Lambda, qui incrémente simplement la valeur spécifiée.

```
// swift-tools-version: 5.9
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
//
// The swift-tools-version declares the minimum version of Swift required to
// build this package.

import PackageDescription

let package = Package(
    name: "increment",
    // Let Xcode know the minimum Apple platforms supported.
    platforms: [
        .macOS(.v13)
    ],
    dependencies: [
        // Dependencies declare other packages that this package depends on.
        .package(
            url: "https://github.com/swift-server/swift-aws-lambda-runtime.git",
            branch: "main"),
    ],
    targets: [
        // Targets are the basic building blocks of a package, defining a module
 or a test suite.
        // Targets can depend on other targets in this package and products
        // from dependencies.
        .executableTarget(
            name: "increment",
            dependencies: [
                .product(name: "AWSLambdaRuntime", package: "swift-aws-lambda-
runtime"),
            ],
            path: "Sources"
        )
    ]
)

import Foundation
import AWSLambdaRuntime

/// Represents the contents of the requests being received from the client.
/// This structure must be `Decodable` to indicate that its initializer
/// converts an external representation into this type.
```

```
struct Request: Decodable, Sendable {
    /// The action to perform.
    let action: String
    /// The number to act upon.
    let number: Int
}

/// The contents of the response sent back to the client. This must be
/// `Encodable`.
struct Response: Encodable, Sendable {
    /// The resulting value after performing the action.
    let answer: Int?
}


/// The Lambda function body.
///
/// - Parameters:
///   - event: The `Request` describing the request made by the
///     client.
///   - context: A `LambdaContext` describing the context in
///     which the lambda function is running.
///
/// - Returns: A `Response` object that will be encoded to JSON and sent
///   to the client by the Lambda runtime.
let incrementLambdaRuntime = LambdaRuntime {
        (event: Request, context: LambdaContext) -> Response in
    let action = event.action
    var answer: Int?

    if action != "increment" {
        context.logger.error("Unrecognized operation: \"\(action)\". The only
 supported action is \"increment\".")
    } else {
        answer = event.number + 1
        context.logger.info("The calculated answer is \(answer!).")
    }

    let response = Response(answer: answer)
    return response
}

// Run the Lambda runtime code.
```

```
try await incrementLambdaRuntime.run()
```

Définissez la deuxième fonction Lambda, qui effectue une opération arithmétique sur deux nombres.

```
// swift-tools-version: 5.9
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
//
// The swift-tools-version declares the minimum version of Swift required to
// build this package.

import PackageDescription

let package = Package(
    name: "calculator",
    // Let Xcode know the minimum Apple platforms supported.
    platforms: [
        .macOS(.v13)
    ],
    dependencies: [
        // Dependencies declare other packages that this package depends on.
        .package(
            url: "https://github.com/swift-server/swift-aws-lambda-runtime.git",
            branch: "main"),
    ],
    targets: [
        // Targets are the basic building blocks of a package, defining a module
 or a test suite.
        // Targets can depend on other targets in this package and products
        // from dependencies.
        .executableTarget(
            name: "calculator",
            dependencies: [
                .product(name: "AWSLambdaRuntime", package: "swift-aws-lambda-
runtime"),
            ],
            path: "Sources"
        )
    ]
)
```

```
import Foundation
import AWSLambdaRuntime

/// Represents the contents of the requests being received from the client.
/// This structure must be `Decodable` to indicate that its initializer
/// converts an external representation into this type.
struct Request: Decodable, Sendable {
    /// The action to perform.
    let action: String
    /// The first number to act upon.
    let x: Int
    /// The second number to act upon.
    let y: Int
}

/// A dictionary mapping operation names to closures that perform that
/// operation and return the result.
let actions = [
    "plus": { (x: Int, y: Int) -> Int in
        return x + y
    },
    "minus": { (x: Int, y: Int) -> Int in
        return x - y
    },
    "times": { (x: Int, y: Int) -> Int in
        return x * y
    },
    "divided-by": { (x: Int, y: Int) -> Int in
        return x / y
    }
]

/// The contents of the response sent back to the client. This must be
/// `Encodable`.
struct Response: Encodable, Sendable {
    /// The resulting value after performing the action.
    let answer: Int?
}



/// The Lambda function's entry point. Called by the Lambda runtime.
///
/// - Parameters:
///   - event: The `Request` describing the request made by the
```

```
///     client.
///   - context: A `LambdaContext` describing the context in
///     which the lambda function is running.
///
/// - Returns: A `Response` object that will be encoded to JSON and sent
///   to the client by the Lambda runtime.
let calculatorLambdaRuntime = LambdaRuntime {
        (_ event: Request, context: LambdaContext) -> Response in
    let action = event.action
    var answer: Int?
    var actionFunc: ((Int, Int) -> Int)?

    // Get the closure to run to perform the calculation.

    actionFunc = await actions[action]

    guard let actionFunc else {
        context.logger.error("Unrecognized operation '\(action)\'")
        return Response(answer: nil)
    }

    // Perform the calculation and return the answer.

    answer = actionFunc(event.x, event.y)

    guard let answer else {
        context.logger.error("Error computing \(event.x) \(action) \(event.y)")
    }
    context.logger.info("\(event.x) \(action) \(event.y) = \(answer)")

    return Response(answer: answer)
}

try await calculatorLambdaRuntime.run()
```

Définissez le programme principal qui invoquera les deux fonctions Lambda.

```
// swift-tools-version: 5.9
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
//
// The swift-tools-version declares the minimum version of Swift required to
```

```
// build this package.

import PackageDescription

let package = Package(
    name: "lambda-basics",
    // Let Xcode know the minimum Apple platforms supported.
    platforms: [
        .macOS(.v13)
    ],
    dependencies: [
        // Dependencies declare other packages that this package depends on.
        .package(
            url: "https://github.com/awslabs/aws-sdk-swift",
            from: "1.0.0"),
        .package(
            url: "https://github.com/apple/swift-argument-parser.git",
            branch: "main"
        )
    ],
    targets: [
        // Targets are the basic building blocks of a package, defining a module
 or a test suite.
        // Targets can depend on other targets in this package and products
        // from dependencies.
        .executableTarget(
            name: "lambda-basics",
            dependencies: [
                .product(name: "AWSLambda", package: "aws-sdk-swift"),
                .product(name: "AWSIAM", package: "aws-sdk-swift"),
                .product(name: "ArgumentParser", package: "swift-argument-
parser")
            ],
            path: "Sources"
        )
    ]
)

//
/// An example demonstrating a variety of important AWS Lambda functions.

import ArgumentParser
import AWSIAM
import SmithyWaitersAPI
```

```
import AWSClientRuntime
import AWSLambda
import Foundation

/// Represents the contents of the requests being received from the client.
/// This structure must be `Decodable` to indicate that its initializer
/// converts an external representation into this type.
struct IncrementRequest: Encodable, Decodable, Sendable {
    /// The action to perform.
    let action: String
    /// The number to act upon.
    let number: Int
}

struct Response: Encodable, Decodable, Sendable {
    /// The resulting value after performing the action.
    let answer: Int?
}

struct CalculatorRequest: Encodable, Decodable, Sendable {
    /// The action to perform.
    let action: String
    /// The first number to act upon.
    let x: Int
    /// The second number to act upon.
    let y: Int
}

let exampleName = "SwiftLambdaRoleExample"
let basicsFunctionName = "lambda-basics-function"

/// The ARN of the standard IAM policy for execution of Lambda functions.
let policyARN = "arn:aws:iam::aws:policy/service-role/
AWSLambdaBasicExecutionRole"

struct ExampleCommand: ParsableCommand {
    // -MARK: Command arguments
    @Option(help: "Name of the IAM Role to use for the Lambda functions")
    var role = exampleName
    @Option(help: "Zip archive containing the 'increment' lambda function")
    var incpath: String
    @Option(help: "Zip archive containing the 'calculator' lambda function")
    var calcpath: String
    @Option(help: "Name of the Amazon S3 Region to use (default: us-east-1)")
```

```
    var region = "us-east-1"

    static var configuration = CommandConfiguration(
        commandName: "lambda-basics",
        abstract: """
        This example demonstrates several common operations using AWS Lambda.
        """,
        discussion: """
        """
    )

    /// Returns the specified IAM role object.
    ///
    /// - Parameters:
    ///   - iamClient: `IAMClient` to use when looking for the role.
    ///   - roleName: The name of the role to check.
    ///
    /// - Returns: The `IAMClientTypes.Role` representing the specified role.
    func getRole(iamClient: IAMClient, roleName: String) async throws
                -> IAMClientTypes.Role {
        do {
            let roleOutput = try await iamClient.getRole(
                input: GetRoleInput(
                    roleName: roleName
                )
            )

            guard let role = roleOutput.role else {
                throw ExampleError.roleNotFound
            }
            return role
        } catch {
            throw ExampleError.roleNotFound
        }
    }

    /// Create the AWS IAM role that will be used to access AWS Lambda.
    ///
    /// - Parameters:
    ///   - iamClient: The AWS `IAMClient` to use.
    ///   - roleName: The name of the AWS IAM role to use for Lambda.
    ///
    /// - Throws: `ExampleError.roleCreateError`
    ///
```

```
    /// - Returns: The `IAMClientTypes.Role` struct that describes the new role.
    func createRoleForLambda(iamClient: IAMClient, roleName: String) async throws
-> IAMClientTypes.Role {
        let output = try await iamClient.createRole(
            input: CreateRoleInput(
                assumeRolePolicyDocument:
                """
                {
                    "Version":"2012-10-17",
                    "Statement": [
                        {
                            "Effect": "Allow",
                            "Principal": {"Service": "lambda.amazonaws.com"},
                            "Action": "sts:AssumeRole"
                        }
                    ]
                }
                """,
                roleName: roleName
            )
        )

        guard let role = output.role else {
            throw ExampleError.roleCreateError
        }

        // Wait for the role to be ready for use.

        _ = try await iamClient.waitUntilRoleExists(
            options: WaiterOptions(
                maxWaitTime: 20,
                minDelay: 0.5,
                maxDelay: 2
            ),
            input: GetRoleInput(roleName: roleName)
        )

        return role
    }

    /// Detect whether or not the AWS Lambda function with the specified name
    /// exists, by requesting its function information.
    ///
    /// - Parameters:
```

```
    ///   - lambdaClient: The `LambdaClient` to use.
    ///   - name: The name of the AWS Lambda function to find.
    ///
    /// - Returns: `true` if the Lambda function exists. Otherwise `false`.
    func doesLambdaFunctionExist(lambdaClient: LambdaClient, name: String) async
-> Bool {
        do {
            _ = try await lambdaClient.getFunction(
                input: GetFunctionInput(functionName: name)
            )
        } catch {
            return false
        }

        return true
    }

    /// Create the specified AWS Lambda function.
    ///
    /// - Parameters:
    ///   - lambdaClient: The `LambdaClient` to use.
    ///   - functionName: The name of the AWS Lambda function to create.
    ///   - roleArn: The ARN of the role to apply to the function.
    ///   - path: The path of the Zip archive containing the function.
    ///
    /// - Returns: `true` if the AWS Lambda was successfully created; `false`
    ///   if it wasn't.
    func createFunction(lambdaClient: LambdaClient, functionName: String,
                                roleArn: String?, path: String) async throws ->
Bool {
        do {
            // Read the Zip archive containing the AWS Lambda function.

            let zipUrl = URL(fileURLWithPath: path)
            let zipData = try Data(contentsOf: zipUrl)

            // Create the AWS Lambda function that runs the specified code,
            // using the name given on the command line. The Lambda function
            // will run using the Amazon Linux 2 runtime.

            _ = try await lambdaClient.createFunction(
                input: CreateFunctionInput(
                    code: LambdaClientTypes.FunctionCode(zipFile: zipData),
                    functionName: functionName,
```

```
                    handler: "handle",
                    role: roleArn,
                    runtime: .providedal2
                )
            )
        } catch {
            print("*** Error creating Lambda function:")
            dump(error)
            return false
        }

        // Wait for a while to be sure the function is done being created.

        let output = try await lambdaClient.waitUntilFunctionActiveV2(
            options: WaiterOptions(
                maxWaitTime: 20,
                minDelay: 0.5,
                maxDelay: 2
            ),
            input: GetFunctionInput(functionName: functionName)
        )

        switch output.result {
            case .success:
                return true
            case .failure:
                return false
        }
    }

    /// Update the AWS Lambda function with new code to run when the function
    /// is invoked.
    ///
    /// - Parameters:
    ///   - lambdaClient: The `LambdaClient` to use.
    ///   - functionName: The name of the AWS Lambda function to update.
    ///   - path: The pathname of the Zip file containing the packaged Lambda
    ///     function.
    /// - Throws: `ExampleError.zipFileReadError`
    /// - Returns: `true` if the function's code is updated successfully.
    ///   Otherwise, returns `false`.
    func updateFunctionCode(lambdaClient: LambdaClient, functionName: String,
                            path: String) async throws -> Bool {
        let zipUrl = URL(fileURLWithPath: path)
```

```
        let zipData: Data

        // Read the function's Zip file.

        do {
            zipData = try Data(contentsOf: zipUrl)
        } catch {
            throw ExampleError.zipFileReadError
        }

        // Update the function's code and wait for the updated version to be
        // ready for use.

        do {
            _ = try await lambdaClient.updateFunctionCode(
                input: UpdateFunctionCodeInput(
                    functionName: functionName,
                    zipFile: zipData
                )
            )
        } catch {
            return false
        }

        let output = try await lambdaClient.waitUntilFunctionUpdatedV2(
            options: WaiterOptions(
                maxWaitTime: 20,
                minDelay: 0.5,
                maxDelay: 2
            ),
            input: GetFunctionInput(
                functionName: functionName
            )
        )

        switch output.result {
            case .success:
                return true
            case .failure:
                return false
        }
    }

    /// Tell the server-side component to log debug output by setting its
```

```
    /// environment's `LOG_LEVEL` to `DEBUG`.
    ///
    /// - Parameters:
    ///   - lambdaClient: The `LambdaClient` to use.
    ///   - functionName: The name of the AWS Lambda function to enable debug
    ///     logging for.
    ///
    /// - Throws: `ExampleError.environmentResponseMissingError`,
    ///   `ExampleError.updateFunctionConfigurationError`,
    ///   `ExampleError.environmentVariablesMissingError`,
    ///   `ExampleError.logLevelIncorrectError`,
    ///   `ExampleError.updateFunctionConfigurationError`
    func enableDebugLogging(lambdaClient: LambdaClient, functionName: String)
async throws {
        let envVariables = [
            "LOG_LEVEL": "DEBUG"
        ]
        let environment = LambdaClientTypes.Environment(variables: envVariables)

        do {
            let output = try await lambdaClient.updateFunctionConfiguration(
                input: UpdateFunctionConfigurationInput(
                    environment: environment,
                    functionName: functionName
                )
            )

            guard let response = output.environment else {
                throw ExampleError.environmentResponseMissingError
            }

            if response.error != nil {
                throw ExampleError.updateFunctionConfigurationError
            }

            guard let retVariables = response.variables else {
                throw ExampleError.environmentVariablesMissingError
            }

            for envVar in retVariables {
                if envVar.key == "LOG_LEVEL" && envVar.value != "DEBUG" {
                    print("*** Log level is not set to DEBUG!")
                    throw ExampleError.logLevelIncorrectError
                }
```

```
            }
        } catch {
            throw ExampleError.updateFunctionConfigurationError
        }
    }

    /// Returns an array containing the names of all AWS Lambda functions
    /// available to the user.
    ///
    /// - Parameter lambdaClient: The `IAMClient` to use.
    ///
    /// - Throws: `ExampleError.listFunctionsError`
    ///
    /// - Returns: An array of lambda function name strings.
    func getFunctionNames(lambdaClient: LambdaClient) async throws -> [String] {
        let pages = lambdaClient.listFunctionsPaginated(
            input: ListFunctionsInput()
        )

        var functionNames: [String] = []

        for try await page in pages {
            guard let functions = page.functions else {
                throw ExampleError.listFunctionsError
            }

            for function in functions {
                functionNames.append(function.functionName ?? "<unknown>")
            }
        }

        return functionNames
    }

    /// Invoke the Lambda function to increment a value.
    ///
    /// - Parameters:
    ///   - lambdaClient: The `IAMClient` to use.
    ///   - number: The number to increment.
    ///
    /// - Throws: `ExampleError.noAnswerReceived`, `ExampleError.invokeError`
    ///
    /// - Returns: An integer number containing the incremented value.
```

```
    func invokeIncrement(lambdaClient: LambdaClient, number: Int) async throws ->
Int {
        do {
            let incRequest = IncrementRequest(action: "increment", number:
number)
            let incData = try! JSONEncoder().encode(incRequest)

            // Invoke the lambda function.

            let invokeOutput = try await lambdaClient.invoke(
                input: InvokeInput(
                    functionName: "lambda-basics-function",
                    payload: incData
                )
            )

            let response = try! JSONDecoder().decode(Response.self,
from:invokeOutput.payload!)

            guard let answer = response.answer else {
                throw ExampleError.noAnswerReceived
            }
            return answer

        } catch {
            throw ExampleError.invokeError
        }
    }

    /// Invoke the calculator Lambda function.
    ///
    /// - Parameters:
    ///   - lambdaClient: The `IAMClient` to use.
    ///   - action: Which arithmetic operation to perform: "plus", "minus",
    ///     "times", or "divided-by".
    ///   - x: The first number to use in the computation.
    ///   - y: The second number to use in the computation.
    ///
    /// - Throws: `ExampleError.noAnswerReceived`, `ExampleError.invokeError`
    ///
    /// - Returns: The computed answer as an `Int`.
    func invokeCalculator(lambdaClient: LambdaClient, action: String, x: Int, y:
Int) async throws -> Int {
        do {
```

```
            let calcRequest = CalculatorRequest(action: action, x: x, y: y)
            let calcData = try! JSONEncoder().encode(calcRequest)

            // Invoke the lambda function.

            let invokeOutput = try await lambdaClient.invoke(
                input: InvokeInput(
                    functionName: "lambda-basics-function",
                    payload: calcData
                )
            )

            let response = try! JSONDecoder().decode(Response.self,
from:invokeOutput.payload!)

            guard let answer = response.answer else {
                throw ExampleError.noAnswerReceived
            }
            return answer

        } catch {
            throw ExampleError.invokeError
        }

    }

    /// Perform the example's tasks.
    func basics() async throws {
        let iamClient = try await IAMClient(
            config: IAMClient.IAMClientConfig(region: region)
        )

        let lambdaClient = try await LambdaClient(
            config: LambdaClient.LambdaClientConfig(region: region)
        )

        /// The IAM role to use for the example.
        var iamRole: IAMClientTypes.Role

        // Look for the specified role. If it already exists, use it. If not,
        // create it and attach the desired policy to it.

        do {
            iamRole = try await getRole(iamClient: iamClient, roleName: role)
```

```
        } catch ExampleError.roleNotFound {
            // The role wasn't found, so create it and attach the needed
            // policy.

            iamRole = try await createRoleForLambda(iamClient: iamClient,
roleName: role)

            do {
                _ = try await iamClient.attachRolePolicy(
                    input: AttachRolePolicyInput(policyArn: policyARN, roleName:
role)
                )
            } catch {
                throw ExampleError.policyError
            }
        }

        // Give the policy time to attach to the role.

        sleep(5)

        // Look to see if the function already exists. If it does, throw an
        // error.

        if await doesLambdaFunctionExist(lambdaClient: lambdaClient, name:
basicsFunctionName) {
            throw ExampleError.functionAlreadyExists
        }

        // Create, then invoke, the "increment" version of the calculator
        // function.

        print("Creating the increment Lambda function...")
        if try await createFunction(lambdaClient: lambdaClient, functionName:
basicsFunctionName,
                                    roleArn: iamRole.arn, path: incpath) {
            print("Running increment function calls...")
            for number in 0...4 {
                do {
                    let answer = try await invokeIncrement(lambdaClient:
lambdaClient, number: number)
                    print("Increment \(number) = \(answer)")
                } catch {
```

```
                    print("Error incrementing \(number): ",
error.localizedDescription)
                }
            }
        } else {
            print("*** Failed to create the increment function.")
        }

        // Enable debug logging.

        print("\nEnabling debug logging...")
        try await enableDebugLogging(lambdaClient: lambdaClient, functionName:
basicsFunctionName)

        // Change it to a basic arithmetic calculator. Then invoke it a few
        // times.

        print("\nReplacing the Lambda function with a calculator...")

        if try await updateFunctionCode(lambdaClient: lambdaClient, functionName:
basicsFunctionName,
                                        path: calcpath) {
            print("Running calculator function calls...")
            for x in [6, 10] {
                for y in [2, 4] {
                    for action in ["plus", "minus", "times", "divided-by"] {
                        do {
                            let answer = try await invokeCalculator(lambdaClient:
lambdaClient, action: action, x: x, y: y)
                            print("\(x) \(action) \(y) = \(answer)")
                        } catch {
                            print("Error calculating \(x) \(action) \(y): ",
error.localizedDescription)
                        }
                    }
                }
            }
        }

        // List all lambda functions.

        let functionNames = try await getFunctionNames(lambdaClient:
lambdaClient)
```

```
        if functionNames.count > 0 {
            print("\nAWS Lambda functions available on your account:")
            for name in functionNames {
                print("  \(name)")
            }
        }

        // Delete the lambda function.

        print("Deleting lambda function...")

        do {
            _ = try await lambdaClient.deleteFunction(
                input: DeleteFunctionInput(
                    functionName: "lambda-basics-function"
                )
            )
        } catch {
            print("Error: Unable to delete the function.")
        }

        // Detach the role from the policy, then delete the role.

        print("Deleting the AWS IAM role...")

        do {
            _ = try await iamClient.detachRolePolicy(
                input: DetachRolePolicyInput(
                    policyArn: policyARN,
                    roleName: role
                )
            )
            _ = try await iamClient.deleteRole(
                input: DeleteRoleInput(
                    roleName: role
                )
            )
        } catch {
            throw ExampleError.deleteRoleError
        }
    }
}

// -MARK: - Entry point
```

```
/// The program's asynchronous entry point.
@main
struct Main {
    static func main() async {
        let args = Array(CommandLine.arguments.dropFirst())

        do {
            let command = try ExampleCommand.parse(args)
            try await command.basics()
        } catch {
            ExampleCommand.exit(withError: error)
        }
    }
}


/// Errors thrown by the example's functions.
enum ExampleError: Error {
    /// An AWS Lambda function with the specified name already exists.
    case functionAlreadyExists
    /// The specified role doesn't exist.
    case roleNotFound
    /// Unable to create the role.
    case roleCreateError
    /// Unable to delete the role.
    case deleteRoleError
    /// Unable to attach a policy to the role.
    case policyError
    /// Unable to get the executable directory.
    case executableNotFound
    /// An error occurred creating a lambda function.
    case createLambdaError
    /// An error occurred invoking the lambda function.
    case invokeError
    /// No answer received from the invocation.
    case noAnswerReceived
    /// Unable to list the AWS Lambda functions.
    case listFunctionsError
    /// Unable to update the AWS Lambda function.
    case updateFunctionError
    /// Unable to update the function configuration.
    case updateFunctionConfigurationError
    /// The environment response is missing after an
```

```
    /// UpdateEnvironmentConfiguration attempt.
    case environmentResponseMissingError
    /// The environment variables are missing from the EnvironmentResponse and
    /// no errors occurred.
    case environmentVariablesMissingError
    /// The log level is incorrect after attempting to set it.
    case logLevelIncorrectError
    /// Unable to load the AWS Lambda function's Zip file.
    case zipFileReadError

    var errorDescription: String? {
        switch self {
        case .functionAlreadyExists:
            return "An AWS Lambda function with that name already exists."
        case .roleNotFound:
            return "The specified role doesn't exist."
        case .deleteRoleError:
            return "Unable to delete the AWS IAM role."
        case .roleCreateError:
            return "Unable to create the specified role."
        case .policyError:
            return "An error occurred attaching the policy to the role."
        case .executableNotFound:
            return "Unable to find the executable program directory."
        case .createLambdaError:
            return "An error occurred creating a lambda function."
        case .invokeError:
            return "An error occurred invoking a lambda function."
        case .noAnswerReceived:
            return "No answer received from the lambda function."
        case .listFunctionsError:
            return "Unable to list the AWS Lambda functions."
        case .updateFunctionError:
            return "Unable to update the AWS lambda function."
        case .updateFunctionConfigurationError:
            return "Unable to update the AWS lambda function configuration."
        case .environmentResponseMissingError:
            return "The environment is missing from the response after updating
the function configuration."
        case .environmentVariablesMissingError:
            return "While no error occurred, no environment variables were
returned following function configuration."
        case .logLevelIncorrectError:
```

```
            return "The log level is incorrect after attempting to set it to
 DEBUG."
        case .zipFileReadError:
            return "Unable to read the AWS Lambda function."
        }
    }
}
```

- Pour plus de détails sur l'API, consultez les rubriques suivantes dans la Référence des API du kit AWS SDK pour Swift.
  - CreateFunction
  - DeleteFunction
  - GetFunction
  - Invoke
  - ListFunctions
  - UpdateFunctionCode
  - UpdateFunctionConfiguration

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Actions pour Lambda à l'aide de AWS Kits SDK

Les exemples de code suivants montrent comment effectuer des actions Lambda individuelles avec AWS SDK. Chaque exemple inclut un lien vers GitHub, où vous trouverez des instructions pour configurer et exécuter le code.

Ces extraits appellent l'API Lambda et sont des extraits de code de programmes plus volumineux qui doivent être exécutés en contexte. Vous pouvez voir les actions dans leur contexte dans Scénarios pour Lambda utilisant AWS Kits SDK.

Les exemples suivants incluent uniquement les actions les plus couramment utilisées. Pour obtenir la liste complète, consultez la Référence des API AWS Lambda.

Exemples

- Utilisation de CreateAlias avec une CLI

- Utiliser CreateFunction avec un AWS SDK ou CLI
- Utilisation de DeleteAlias avec une CLI
- Utiliser DeleteFunction avec un AWS SDK ou CLI
- Utilisation de DeleteFunctionConcurrency avec une CLI
- Utilisation de DeleteProvisionedConcurrencyConfig avec une CLI
- Utilisation de GetAccountSettings avec une CLI
- Utilisation de GetAlias avec une CLI
- Utiliser GetFunction avec un AWS SDK ou CLI
- Utilisation de GetFunctionConcurrency avec une CLI
- Utilisation de GetFunctionConfiguration avec une CLI
- Utilisation de GetPolicy avec une CLI
- Utilisation de GetProvisionedConcurrencyConfig avec une CLI
- Utiliser Invoquer avec un AWS SDK ou CLI
- Utiliser ListFunctions avec un AWS SDK ou CLI
- Utilisation de ListProvisionedConcurrencyConfigs avec une CLI
- Utilisation de ListTags avec une CLI
- Utilisation de ListVersionsByFunction avec une CLI
- Utilisation de PublishVersion avec une CLI
- Utilisation de PutFunctionConcurrency avec une CLI
- Utilisation de PutProvisionedConcurrencyConfig avec une CLI
- Utilisation de RemovePermission avec une CLI
- Utilisation de TagResource avec une CLI
- Utilisation de UntagResource avec une CLI
- Utilisation de UpdateAlias avec une CLI
- Utiliser UpdateFunctionCode avec un AWS SDK ou CLI
- Utiliser UpdateFunctionConfiguration avec un AWS SDK ou CLI

Utilisation de **`CreateAlias`** avec une CLI

Les exemples de code suivants illustrent comment utiliser `CreateAlias`.

CLI

AWS CLI

Pour créer un alias de fonction Lambda

L'exemple `create-alias` suivant crée un alias de fonction Lambda nommé `LIVE` qui pointe vers la version 1 de la fonction Lambda `my-function`.

```
aws lambda create-alias \
    --function-name my-function \
    --description "alias for live version of function" \
    --function-version 1 \
    --name LIVE
```

Sortie :

```
{
    "FunctionVersion": "1",
    "Name": "LIVE",
    "AliasArn": "arn:aws:lambda:us-west-2:123456789012:function:my-
function:LIVE",
    "RevisionId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Description": "alias for live version of function"
}
```

Pour plus d'informations, voir Configuration AWS Alias de fonctions Lambda dans le AWS Guide du développeur Lambda.

- Pour plus de détails sur l'API, voir CreateAlias dans AWS CLI Référence de commande.

PowerShell

Outils pour PowerShell V4

Exemple 1 : cet exemple crée un alias Lambda pour une version et une configuration de routage spécifiées afin de déterminer le pourcentage de requêtes d'invocation reçues.

```
New-LMAlias -FunctionName "MylambdaFunction123" -
RoutingConfig_AdditionalVersionWeight @{Name="1";Value="0.6} -Description "Alias
 for version 4" -FunctionVersion 4 -Name "PowershellAlias"
```

- Pour plus de détails sur l'API, voir CreateAlias dans Outils AWS pour PowerShell Référence de l'applet de commande (V4).

Outils pour PowerShell V5

Exemple 1 : cet exemple crée un alias Lambda pour une version et une configuration de routage spécifiées afin de déterminer le pourcentage de requêtes d'invocation reçues.

```
New-LMAlias -FunctionName "MylambdaFunction123" -
RoutingConfig_AdditionalVersionWeight @{Name="1";Value="0.6} -Description "Alias
 for version 4" -FunctionVersion 4 -Name "PowershellAlias"
```

- Pour plus de détails sur l'API, voir CreateAlias dans Outils AWS pour PowerShell Référence de l'applet de commande (V5).

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Utiliser **`CreateFunction`** avec un AWS SDK ou CLI

Les exemples de code suivants illustrent comment utiliser `CreateFunction`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans les exemples de code suivants :

- Principes de base
- Création d'une API REST avec intégration de fonctions proxy
- Création d'un tableau de bord de surveillance avec le nom de fonction comme variable
- Création de votre première fonction sans serveur
- Utilisation de variables de propriété dans les tableaux de bord de surveillance pour surveiller plusieurs fonctions sans serveur

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
/// <summary>
/// Creates a new Lambda function.
/// </summary>
/// <param name="functionName">The name of the function.</param>
/// <param name="s3Bucket">The Amazon Simple Storage Service (Amazon S3)
/// bucket where the zip file containing the code is located.</param>
/// <param name="s3Key">The Amazon S3 key of the zip file.</param>
/// <param name="role">The Amazon Resource Name (ARN) of a role with the
/// appropriate Lambda permissions.</param>
/// <param name="handler">The name of the handler function.</param>
/// <returns>The Amazon Resource Name (ARN) of the newly created
/// Lambda function.</returns>
public async Task<string> CreateLambdaFunctionAsync(
    string functionName,
    string s3Bucket,
    string s3Key,
    string role,
    string handler)
{
    // Defines the location for the function code.
    // S3Bucket - The S3 bucket where the file containing
    //            the source code is stored.
    // S3Key    - The name of the file containing the code.
    var functionCode = new FunctionCode
    {
        S3Bucket = s3Bucket,
        S3Key = s3Key,
    };

    var createFunctionRequest = new CreateFunctionRequest
    {
        FunctionName = functionName,
```

```
            Description = "Created by the Lambda .NET API",
            Code = functionCode,
            Handler = handler,
            Runtime = Runtime.Dotnet6,
            Role = role,
        };

        var reponse = await
_lambdaService.CreateFunctionAsync(createFunctionRequest);
        return reponse.FunctionArn;
    }
```

- Pour plus de détails sur l'API, voir CreateFunction dans AWS SDK pour .NET Référence d'API.

C++

SDK pour C++

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
        Aws::Client::ClientConfiguration clientConfig;
        // Optional: Set to the AWS Region in which the bucket was created
(overrides config file).
        // clientConfig.region = "us-east-1";

    Aws::Lambda::LambdaClient client(clientConfig);

        Aws::Lambda::Model::CreateFunctionRequest request;
        request.SetFunctionName(LAMBDA_NAME);
        request.SetDescription(LAMBDA_DESCRIPTION); // Optional.
#if USE_CPP_LAMBDA_FUNCTION
        request.SetRuntime(Aws::Lambda::Model::Runtime::provided_al2);
        request.SetTimeout(15);
        request.SetMemorySize(128);
```

```
        // Assume the AWS Lambda function was built in Docker with same
 architecture
        // as this code.
#if  defined(__x86_64__)
        request.SetArchitectures({Aws::Lambda::Model::Architecture::x86_64});
#elif defined(__aarch64__)
        request.SetArchitectures({Aws::Lambda::Model::Architecture::arm64});
#else
#error "Unimplemented architecture"
#endif // defined(architecture)
#else
        request.SetRuntime(Aws::Lambda::Model::Runtime::python3_9);
#endif
        request.SetRole(roleArn);
        request.SetHandler(LAMBDA_HANDLER_NAME);
        request.SetPublish(true);
        Aws::Lambda::Model::FunctionCode code;
        std::ifstream ifstream(INCREMENT_LAMBDA_CODE.c_str(),
                               std::ios_base::in | std::ios_base::binary);
        if (!ifstream.is_open()) {
            std::cerr << "Error opening file " << INCREMENT_LAMBDA_CODE << "." <<
 std::endl;

#if USE_CPP_LAMBDA_FUNCTION
            std::cerr
                    << "The cpp Lambda function must be built following the
 instructions in the cpp_lambda/README.md file. "
                    << std::endl;
#endif
            deleteIamRole(clientConfig);
            return false;
        }

        Aws::StringStream buffer;
        buffer << ifstream.rdbuf();

        code.SetZipFile(Aws::Utils::ByteBuffer((unsigned char *)
 buffer.str().c_str(),
                                               buffer.str().length()));
        request.SetCode(code);

        Aws::Lambda::Model::CreateFunctionOutcome outcome =
 client.CreateFunction(
```

```
                request);

        if (outcome.IsSuccess()) {
            std::cout << "The lambda function was successfully created. " <<
 seconds
                      << " seconds elapsed." << std::endl;
            break;
        }

        else {
            std::cerr << "Error with CreateFunction. "
                      << outcome.GetError().GetMessage()
                      << std::endl;
            deleteIamRole(clientConfig);
            return false;
        }
```

- Pour plus de détails sur l'API, voir CreateFunction dans AWS SDK pour C++ Référence d'API.

CLI

AWS CLI

Pour créer une fonction Lambda

L'exemple `create-function` suivant crée une fonction Lambda nommée `my-function`.

```
aws lambda create-function \
    --function-name my-function \
    --runtime nodejs22.x \
    --zip-file fileb://my-function.zip \
    --handler my-function.handler \
    --role arn:aws:iam::123456789012:role/service-role/MyTestFunction-role-
tges6bf4
```

Contenu de `my-function.zip` :

```
This file is a deployment package that contains your function code and any
 dependencies.
```

Sortie :

```
{
    "TracingConfig": {
        "Mode": "PassThrough"
    },
    "CodeSha256": "PFn4S+er27qk+UuZSTKEQfNKG/XNn7QJs90mJgq6oH8=",
    "FunctionName": "my-function",
    "CodeSize": 308,
    "RevisionId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "MemorySize": 128,
    "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-function",
    "Version": "$LATEST",
    "Role": "arn:aws:iam::123456789012:role/service-role/MyTestFunction-role-
zgur6bf4",
    "Timeout": 3,
    "LastModified": "2025-10-14T22:26:11.234+0000",
    "Handler": "my-function.handler",
    "Runtime": "nodejs22.x",
    "Description": ""
}
```

Pour plus d'informations, consultez Configurer la mémoire de fonction Lambda dans le Guide du développeur AWS Lambda.

- Pour plus de détails sur l'API, voir CreateFunction dans AWS CLI Référence de commande.

Go

Kit SDK pour Go V2

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import (
 "bytes"
 "context"
 "encoding/json"
```

```
 "errors"
 "log"
 "time"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/service/lambda"
 "github.com/aws/aws-sdk-go-v2/service/lambda/types"
)

// FunctionWrapper encapsulates function actions used in the examples.
// It contains an AWS Lambda service client that is used to perform user actions.
type FunctionWrapper struct {
 LambdaClient *lambda.Client
}



// CreateFunction creates a new Lambda function from code contained in the
 zipPackage
// buffer. The specified handlerName must match the name of the file and function
// contained in the uploaded code. The role specified by iamRoleArn is assumed by
// Lambda and grants specific permissions.
// When the function already exists, types.StateActive is returned.
// When the function is created, a lambda.FunctionActiveV2Waiter is used to wait
 until the
// function is active.
func (wrapper FunctionWrapper) CreateFunction(ctx context.Context, functionName
 string, handlerName string,
 iamRoleArn *string, zipPackage *bytes.Buffer) types.State {
 var state types.State
 _, err := wrapper.LambdaClient.CreateFunction(ctx, &lambda.CreateFunctionInput{
  Code:         &types.FunctionCode{ZipFile: zipPackage.Bytes()},
  FunctionName: aws.String(functionName),
  Role:         iamRoleArn,
  Handler:      aws.String(handlerName),
  Publish:      true,
  Runtime:      types.RuntimePython39,
 })
 if err != nil {
  var resConflict *types.ResourceConflictException
  if errors.As(err, &resConflict) {
   log.Printf("Function %v already exists.\n", functionName)
   state = types.StateActive
  } else {
```

```
    log.Panicf("Couldn't create function %v. Here's why: %v\n", functionName, err)
   }
  } else {
   waiter := lambda.NewFunctionActiveV2Waiter(wrapper.LambdaClient)
   funcOutput, err := waiter.WaitForOutput(ctx, &lambda.GetFunctionInput{
    FunctionName: aws.String(functionName)}, 1*time.Minute)
   if err != nil {
    log.Panicf("Couldn't wait for function %v to be active. Here's why: %v\n",
  functionName, err)
   } else {
    state = funcOutput.Configuration.State
   }
  }
  return state
 }
```

- Pour plus de détails sur l'API, voir CreateFunction dans AWS SDK pour Go Référence d'API.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    /**
     * Creates a new Lambda function in AWS using the AWS Lambda Java API.
     *
     * @param awsLambda    the AWS Lambda client used to interact with the AWS
  Lambda service
     * @param functionName the name of the Lambda function to create
     * @param key          the S3 key of the function code
     * @param bucketName   the name of the S3 bucket containing the function code
     * @param role         the IAM role to assign to the Lambda function
     * @param handler      the fully qualified class name of the function handler
```

```
     * @return the Amazon Resource Name (ARN) of the created Lambda function
     */
    public static String createLambdaFunction(LambdaClient awsLambda,
                                               String functionName,
                                               String key,
                                               String bucketName,
                                               String role,
                                               String handler) {

        try {
            LambdaWaiter waiter = awsLambda.waiter();
            FunctionCode code = FunctionCode.builder()
                .s3Key(key)
                .s3Bucket(bucketName)
                .build();

            CreateFunctionRequest functionRequest =
CreateFunctionRequest.builder()
                .functionName(functionName)
                .description("Created by the Lambda Java API")
                .code(code)
                .handler(handler)
                .runtime(Runtime.JAVA17)
                .role(role)
                .build();

            // Create a Lambda function using a waiter
            CreateFunctionResponse functionResponse =
awsLambda.createFunction(functionRequest);
            GetFunctionRequest getFunctionRequest = GetFunctionRequest.builder()
                .functionName(functionName)
                .build();
            WaiterResponse<GetFunctionResponse> waiterResponse =
waiter.waitUntilFunctionExists(getFunctionRequest);
            waiterResponse.matched().response().ifPresent(System.out::println);
            return functionResponse.functionArn();

        } catch (LambdaException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
        return "";
    }
```

- Pour plus de détails sur l'API, voir CreateFunction dans AWS SDK for Java 2.x Référence d'API.

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
const createFunction = async (funcName, roleArn) => {
  const client = new LambdaClient({});
  const code = await readFile(`${dirname}../functions/${funcName}.zip`);

  const command = new CreateFunctionCommand({
    Code: { ZipFile: code },
    FunctionName: funcName,
    Role: roleArn,
    Architectures: [Architecture.arm64],
    Handler: "index.handler", // Required when sending a .zip file
    PackageType: PackageType.Zip, // Required when sending a .zip file
    Runtime: Runtime.nodejs16x, // Required when sending a .zip file
  });

  return client.send(command);
};
```

- Pour plus de détails sur l'API, voir CreateFunction dans AWS SDK pour JavaScript Référence d'API.

Kotlin

SDK pour Kotlin

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
suspend fun createNewFunction(
    myFunctionName: String,
    s3BucketName: String,
    myS3Key: String,
    myHandler: String,
    myRole: String,
): String? {
    val functionCode =
        FunctionCode {
            s3Bucket = s3BucketName
            s3Key = myS3Key
        }

    val request =
        CreateFunctionRequest {
            functionName = myFunctionName
            code = functionCode
            description = "Created by the Lambda Kotlin API"
            handler = myHandler
            role = myRole
            runtime = Runtime.Java17
        }

    LambdaClient { region = "us-east-1" }.use { awsLambda ->
        val functionResponse = awsLambda.createFunction(request)
        awsLambda.waitUntilFunctionActive {
            functionName = myFunctionName
        }
        return functionResponse.functionArn
    }
}
```

- Pour plus de détails sur l'API, voir CreateFunction dans AWS Référence du SDK pour l'API Kotlin.

PHP

Kit SDK pour PHP

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    public function createFunction($functionName, $role, $bucketName, $handler)
    {
        //This assumes the Lambda function is in an S3 bucket.
        return $this->customWaiter(function () use ($functionName, $role,
$bucketName, $handler) {
            return $this->lambdaClient->createFunction([
                'Code' => [
                    'S3Bucket' => $bucketName,
                    'S3Key' => $functionName,
                ],
                'FunctionName' => $functionName,
                'Role' => $role['Arn'],
                'Runtime' => 'python3.9',
                'Handler' => "$handler.lambda_handler",
            ]);
        });
    }
```

- Pour plus de détails sur l'API, voir CreateFunction dans AWS SDK pour PHP Référence d'API.

PowerShell

Outils pour PowerShell V4

Exemple 1 : Cet exemple crée une nouvelle fonction C# (dotnetcore1.0 runtime) MyFunction nomméedans AWS Lambda, fournissant les binaires compilés pour la fonction à partir d'un fichier zip sur le système de fichiers local (des chemins relatifs ou absolus peuvent être utilisés). Les fonctions C# Lambda spécifient le gestionnaire de la fonction à l'aide de la désignation AssemblyName: :Namespace.ClassName: :MethodName. Vous devez remplacer les parties du nom de l'assemblage (sans le suffixe .dll), de l'espace de noms, du nom de classe et du nom de méthode de la spécification du gestionnaire de manière appropriée. La nouvelle fonction aura les variables d'environnement « envvar1 » et « envvar2 » configurées à partir des valeurs fournies.

```
Publish-LMFunction -Description "My C# Lambda Function" `
        -FunctionName MyFunction `
        -ZipFilename .\MyFunctionBinaries.zip `
        -Handler "AssemblyName::Namespace.ClassName::MethodName" `
        -Role "arn:aws:iam::123456789012:role/LambdaFullExecRole" `
        -Runtime dotnetcore1.0 `
        -Environment_Variable @{ "envvar1"="value";"envvar2"="value" }
```

Sortie :

```
CodeSha256       : /NgBMd...gq71I=
CodeSize         : 214784
DeadLetterConfig :
Description      : My C# Lambda Function
Environment      : Amazon.Lambda.Model.EnvironmentResponse
FunctionArn      : arn:aws:lambda:us-west-2:123456789012:function:ToUpper
FunctionName     : MyFunction
Handler          : AssemblyName::Namespace.ClassName::MethodName
KMSKeyArn        :
LastModified     : 2016-12-29T23:50:14.207+0000
MemorySize       : 128
Role             : arn:aws:iam::123456789012:role/LambdaFullExecRole
Runtime          : dotnetcore1.0
Timeout          : 3
Version          : $LATEST
VpcConfig        :
```

Exemple 2 : cet exemple est similaire au précédent, sauf que les fichiers binaires des fonctions sont d'abord chargés dans un compartiment Amazon S3 (qui doit se trouver dans la même région que la fonction Lambda prévue) et que l'objet S3 obtenu est ensuite référencé lors de la création de la fonction.

```
Write-S3Object -BucketName amzn-s3-demo-bucket -Key MyFunctionBinaries.zip -
File .\MyFunctionBinaries.zip
Publish-LMFunction -Description "My C# Lambda Function" `
        -FunctionName MyFunction `
        -BucketName amzn-s3-demo-bucket `
        -Key MyFunctionBinaries.zip `
        -Handler "AssemblyName::Namespace.ClassName::MethodName" `
        -Role "arn:aws:iam::123456789012:role/LambdaFullExecRole" `
        -Runtime dotnetcore1.0 `
        -Environment_Variable @{ "envvar1"="value";"envvar2"="value" }
```

- Pour plus de détails sur l'API, voir CreateFunction dans Outils AWS pour PowerShell Référence de l'applet de commande (V4).

Outils pour PowerShell V5

Exemple 1 : Cet exemple crée une nouvelle fonction C# (dotnetcore1.0 runtime) MyFunction nomméedans AWS Lambda, fournissant les binaires compilés pour la fonction à partir d'un fichier zip sur le système de fichiers local (des chemins relatifs ou absolus peuvent être utilisés). Les fonctions C# Lambda spécifient le gestionnaire de la fonction à l'aide de la désignation AssemblyName: :Namespace.ClassName: :MethodName. Vous devez remplacer les parties du nom de l'assemblage (sans le suffixe .dll), de l'espace de noms, du nom de classe et du nom de méthode de la spécification du gestionnaire de manière appropriée. La nouvelle fonction aura les variables d'environnement « envvar1 » et « envvar2 » configurées à partir des valeurs fournies.

```
Publish-LMFunction -Description "My C# Lambda Function" `
        -FunctionName MyFunction `
        -ZipFilename .\MyFunctionBinaries.zip `
        -Handler "AssemblyName::Namespace.ClassName::MethodName" `
        -Role "arn:aws:iam::123456789012:role/LambdaFullExecRole" `
        -Runtime dotnetcore1.0 `
        -Environment_Variable @{ "envvar1"="value";"envvar2"="value" }
```

Sortie :

```
CodeSha256       : /NgBMd...gq71I=
CodeSize         : 214784
DeadLetterConfig :
Description      : My C# Lambda Function
Environment      : Amazon.Lambda.Model.EnvironmentResponse
FunctionArn      : arn:aws:lambda:us-west-2:123456789012:function:ToUpper
FunctionName     : MyFunction
Handler          : AssemblyName::Namespace.ClassName::MethodName
KMSKeyArn        :
LastModified     : 2016-12-29T23:50:14.207+0000
MemorySize       : 128
Role             : arn:aws:iam::123456789012:role/LambdaFullExecRole
Runtime          : dotnetcore1.0
Timeout          : 3
Version          : $LATEST
VpcConfig        :
```

Exemple 2 : cet exemple est similaire au précédent, sauf que les fichiers binaires des fonctions sont d'abord chargés dans un compartiment Amazon S3 (qui doit se trouver dans la même région que la fonction Lambda prévue) et que l'objet S3 obtenu est ensuite référencé lors de la création de la fonction.

```
Write-S3Object -BucketName amzn-s3-demo-bucket -Key MyFunctionBinaries.zip -
File .\MyFunctionBinaries.zip
Publish-LMFunction -Description "My C# Lambda Function" `
        -FunctionName MyFunction `
        -BucketName amzn-s3-demo-bucket `
        -Key MyFunctionBinaries.zip `
        -Handler "AssemblyName::Namespace.ClassName::MethodName" `
        -Role "arn:aws:iam::123456789012:role/LambdaFullExecRole" `
        -Runtime dotnetcore1.0 `
        -Environment_Variable @{ "envvar1"="value";"envvar2"="value" }
```

- Pour plus de détails sur l'API, voir CreateFunction dans Outils AWS pour PowerShell Référence de l'applet de commande (V5).

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class LambdaWrapper:
    def __init__(self, lambda_client, iam_resource):
        self.lambda_client = lambda_client
        self.iam_resource = iam_resource


    def create_function(
        self, function_name, handler_name, iam_role, deployment_package
    ):
        """
        Deploys a Lambda function.

        :param function_name: The name of the Lambda function.
        :param handler_name: The fully qualified name of the handler function.
 This
                             must include the file name and the function name.
        :param iam_role: The IAM role to use for the function.
        :param deployment_package: The deployment package that contains the
 function
                                   code in .zip format.
        :return: The Amazon Resource Name (ARN) of the newly created function.
        """
        try:
            response = self.lambda_client.create_function(
                FunctionName=function_name,
                Description="AWS Lambda doc example",
                Runtime="python3.9",
                Role=iam_role.arn,
                Handler=handler_name,
                Code={"ZipFile": deployment_package},
                Publish=True,
            )
```

```
            function_arn = response["FunctionArn"]
            waiter = self.lambda_client.get_waiter("function_active_v2")
            waiter.wait(FunctionName=function_name)
            logger.info(
                "Created function '%s' with ARN: '%s'.",
                function_name,
                response["FunctionArn"],
            )
        except ClientError:
            logger.error("Couldn't create function %s.", function_name)
            raise
        else:
            return function_arn
```

- Pour plus de détails sur l'API, voir CreateFunction dans AWS Référence de l'API du SDK pour Python (Boto3).

Ruby

Kit SDK pour Ruby

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class LambdaWrapper
  attr_accessor :lambda_client, :cloudwatch_client, :iam_client

  def initialize
    @lambda_client = Aws::Lambda::Client.new
    @cloudwatch_client = Aws::CloudWatchLogs::Client.new(region: 'us-east-1')
    @iam_client = Aws::IAM::Client.new(region: 'us-east-1')
    @logger = Logger.new($stdout)
    @logger.level = Logger::WARN
  end

  # Deploys a Lambda function.
```

```
  #
  # @param function_name: The name of the Lambda function.
  # @param handler_name: The fully qualified name of the handler function.
  # @param role_arn: The IAM role to use for the function.
  # @param deployment_package: The deployment package that contains the function
code in .zip format.
  # @return: The Amazon Resource Name (ARN) of the newly created function.
  def create_function(function_name, handler_name, role_arn, deployment_package)
    response = @lambda_client.create_function({
                                                role: role_arn.to_s,
                                                function_name: function_name,
                                                handler: handler_name,
                                                runtime: 'ruby2.7',
                                                code: {
                                                  zip_file: deployment_package
                                                },
                                                environment: {
                                                  variables: {
                                                    'LOG_LEVEL' => 'info'
                                                  }
                                                }
                                              })
    @lambda_client.wait_until(:function_active_v2, { function_name:
function_name }) do |w|
      w.max_attempts = 5
      w.delay = 5
    end
    response
  rescue Aws::Lambda::Errors::ServiceException => e
    @logger.error("There was an error creating #{function_name}:\n #{e.message}")
  rescue Aws::Waiters::Errors::WaiterFailed => e
    @logger.error("Failed waiting for #{function_name} to activate:\n
#{e.message}")
  end
```

- Pour plus de détails sur l'API, voir CreateFunction dans AWS SDK pour Ruby Référence d'API.

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    /**
     * Create a function, uploading from a zip file.
     */
    pub async fn create_function(&self, zip_file: PathBuf) -> Result<String,
anyhow::Error> {
        let code = self.prepare_function(zip_file, None).await?;

        let key = code.s3_key().unwrap().to_string();

        let role = self.create_role().await.map_err(|e| anyhow!(e))?;

        info!("Created iam role, waiting 15s for it to become active");
        tokio::time::sleep(Duration::from_secs(15)).await;

        info!("Creating lambda function {}", self.lambda_name);
        let _ = self
            .lambda_client
            .create_function()
            .function_name(self.lambda_name.clone())
            .code(code)
            .role(role.arn())
            .runtime(aws_sdk_lambda::types::Runtime::Providedal2)
            .handler("_unused")
            .send()
            .await
            .map_err(anyhow::Error::from)?;

        self.wait_for_function_ready().await?;

        self.lambda_client
            .publish_version()
            .function_name(self.lambda_name.clone())
```

```
            .send()
            .await?;

        Ok(key)
    }

    /**
     * Upload function code from a path to a zip file.
     * The zip file must have an AL2 Linux-compatible binary called `bootstrap`.
     * The easiest way to create such a zip is to use `cargo lambda build --
output-format Zip`.
     */
    async fn prepare_function(
        &self,
        zip_file: PathBuf,
        key: Option<String>,
    ) -> Result<FunctionCode, anyhow::Error> {
        let body = ByteStream::from_path(zip_file).await?;

        let key = key.unwrap_or_else(|| format!("{}_code", self.lambda_name));

        info!("Uploading function code to s3://{}/{}", self.bucket, key);
        let _ = self
            .s3_client
            .put_object()
            .bucket(self.bucket.clone())
            .key(key.clone())
            .body(body)
            .send()
            .await?;

        Ok(FunctionCode::builder()
            .s3_bucket(self.bucket.clone())
            .s3_key(key)
            .build())
    }
```

- Pour plus de détails sur l'API, voir CreateFunction dans AWS Référence de l'API SDK pour Rust.

SAP ABAP

Kit SDK pour SAP ABAP

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
   TRY.
       lo_lmd->createfunction(
           iv_functionname = iv_function_name
           iv_runtime = `python3.9`
           iv_role = iv_role_arn
           iv_handler = iv_handler
           io_code = io_zip_file
           iv_description = 'AWS Lambda code example' ).
       MESSAGE 'Lambda function created.' TYPE 'I'.
     CATCH /aws1/cx_lmdcodesigningcfgno00.
       MESSAGE 'Code signing configuration does not exist.' TYPE 'E'.
     CATCH /aws1/cx_lmdcodestorageexcdex.
       MESSAGE 'Maximum total code size per account exceeded.' TYPE 'E'.
     CATCH /aws1/cx_lmdcodeverification00.
       MESSAGE 'Code signature failed one or more validation checks for
signature mismatch or expiration.' TYPE 'E'.
     CATCH /aws1/cx_lmdinvalidcodesigex.
       MESSAGE 'Code signature failed the integrity check.' TYPE 'E'.
     CATCH /aws1/cx_lmdinvparamvalueex.
       MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
     CATCH /aws1/cx_lmdresourceconflictex.
       MESSAGE 'Resource already exists or another operation is in progress.'
TYPE 'E'.
     CATCH /aws1/cx_lmdresourcenotfoundex.
       MESSAGE 'The requested resource does not exist.' TYPE 'E'.
     CATCH /aws1/cx_lmdserviceexception.
       MESSAGE 'An internal problem was encountered by the AWS Lambda service.'
TYPE 'E'.
     CATCH /aws1/cx_lmdtoomanyrequestsex.
       MESSAGE 'The maximum request throughput was reached.' TYPE 'E'.
   ENDTRY.
```

- Pour plus de détails sur l'API, voir CreateFunction dans AWS Référence du SDK pour l'API SAP ABAP.

Swift

Kit SDK pour Swift

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import AWSClientRuntime
import AWSLambda
import Foundation

        do {
            // Read the Zip archive containing the AWS Lambda function.

            let zipUrl = URL(fileURLWithPath: path)
            let zipData = try Data(contentsOf: zipUrl)

            // Create the AWS Lambda function that runs the specified code,
            // using the name given on the command line. The Lambda function
            // will run using the Amazon Linux 2 runtime.

            _ = try await lambdaClient.createFunction(
                input: CreateFunctionInput(
                    code: LambdaClientTypes.FunctionCode(zipFile: zipData),
                    functionName: functionName,
                    handler: "handle",
                    role: roleArn,
                    runtime: .providedal2
                )
            )
        } catch {
            print("*** Error creating Lambda function:")
            dump(error)
            return false
        }
```

- Pour plus de détails sur l'API, voir CreateFunction dans AWS Référence du SDK pour l'API Swift.

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Utilisation de **`DeleteAlias`** avec une CLI

Les exemples de code suivants illustrent comment utiliser `DeleteAlias`.

CLI

AWS CLI

Pour supprimer un alias de fonction Lambda

L'exemple `delete-alias` suivant supprime l'alias nommé `LIVE` de la fonction Lambda `my-function`.

```
aws lambda delete-alias \
    --function-name my-function \
    --name LIVE
```

Cette commande ne produit aucune sortie.

Pour plus d'informations, voir Configuration AWS Alias de fonctions Lambda dans le AWS Guide du développeur Lambda.

- Pour plus de détails sur l'API, voir DeleteAlias dans AWS CLI Référence de commande.

PowerShell

Outils pour PowerShell V4

Exemple 1 : cet exemple supprime l'alias de la fonction Lambda mentionnée dans la commande.

```
Remove-LMAlias -FunctionName "MylambdaFunction123" -Name "NewAlias"
```

- Pour plus de détails sur l'API, voir DeleteAlias dans Outils AWS pour PowerShell Référence de l'applet de commande (V4).

Outils pour PowerShell V5

Exemple 1 : cet exemple supprime l’alias de la fonction Lambda mentionnée dans la commande.

```
Remove-LMAlias -FunctionName "MylambdaFunction123" -Name "NewAlias"
```

- Pour plus de détails sur l'API, voir DeleteAlias dans Outils AWS pour PowerShell Référence de l'applet de commande (V5).

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Utiliser **`DeleteFunction`** avec un AWS SDK ou CLI

Les exemples de code suivants illustrent comment utiliser `DeleteFunction`.

Les exemples d’actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans les exemples de code suivants :

- Principes de base
- Création d'une API REST avec intégration de fonctions proxy
- Création d’un tableau de bord de surveillance avec le nom de fonction comme variable
- Création de votre première fonction sans serveur
- Utilisation de variables de propriété dans les tableaux de bord de surveillance pour surveiller plusieurs fonctions sans serveur

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    /// <summary>
    /// Delete an AWS Lambda function.
    /// </summary>
    /// <param name="functionName">The name of the Lambda function to
    /// delete.</param>
    /// <returns>A Boolean value that indicates the success of the action.</
returns>
    public async Task<bool> DeleteFunctionAsync(string functionName)
    {
        var request = new DeleteFunctionRequest
        {
            FunctionName = functionName,
        };

        var response = await _lambdaService.DeleteFunctionAsync(request);

        // A return value of NoContent means that the request was processed.
        // In this case, the function was deleted, and the return value
        // is intentionally blank.
        return response.HttpStatusCode == System.Net.HttpStatusCode.NoContent;
    }
```

- Pour plus de détails sur l'API, voir DeleteFunction dans AWS SDK pour .NET Référence d'API.

C++

SDK pour C++

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
        Aws::Client::ClientConfiguration clientConfig;
        // Optional: Set to the AWS Region in which the bucket was created
(overrides config file).
        // clientConfig.region = "us-east-1";

    Aws::Lambda::LambdaClient client(clientConfig);

    Aws::Lambda::Model::DeleteFunctionRequest request;
    request.SetFunctionName(LAMBDA_NAME);

    Aws::Lambda::Model::DeleteFunctionOutcome outcome = client.DeleteFunction(
            request);

    if (outcome.IsSuccess()) {
        std::cout << "The lambda function was successfully deleted." <<
std::endl;
    }
    else {
        std::cerr << "Error with Lambda::DeleteFunction. "
                  << outcome.GetError().GetMessage()
                  << std::endl;
    }
```

- Pour plus de détails sur l'API, voir DeleteFunction dans AWS SDK pour C++ Référence d'API.

CLI

AWS CLI

Exemple 1 : pour supprimer une fonction Lambda par nom de fonction

L'exemple `delete-function` suivant supprime la fonction Lambda `my-function` nommée en spécifiant le nom de la fonction.

```
aws lambda delete-function \
    --function-name my-function
```

Cette commande ne produit aucune sortie.

Exemple 2 : pour supprimer une fonction Lambda par ARN de fonction

L'exemple `delete-function` suivant supprime la fonction Lambda nommée `my-function` en spécifiant l'ARN de la fonction.

```
aws lambda delete-function \
    --function-name arn:aws:lambda:us-west-2:123456789012:function:my-function
```

Cette commande ne produit aucune sortie.

Exemple 3 : pour supprimer une fonction Lambda par ARN partiel de fonction

L'exemple `delete-function` suivant supprime la fonction Lambda nommée `my-function` en spécifiant l'ARN partiel de la fonction.

```
aws lambda delete-function \
    --function-name 123456789012:function:my-function
```

Cette commande ne produit aucune sortie.

Pour plus d'informations, consultez Configuration des options de fonction Lambda AWS dans le Guide du développeur AWS .

- Pour plus de détails sur l'API, voir DeleteFunction dans AWS CLI Référence de commande.

Go

Kit SDK pour Go V2

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import (
 "bytes"
 "context"
 "encoding/json"
 "errors"
 "log"
 "time"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/service/lambda"
 "github.com/aws/aws-sdk-go-v2/service/lambda/types"
)

// FunctionWrapper encapsulates function actions used in the examples.
// It contains an AWS Lambda service client that is used to perform user actions.
type FunctionWrapper struct {
 LambdaClient *lambda.Client
}



// DeleteFunction deletes the Lambda function specified by functionName.
func (wrapper FunctionWrapper) DeleteFunction(ctx context.Context, functionName
 string) {
 _, err := wrapper.LambdaClient.DeleteFunction(ctx, &lambda.DeleteFunctionInput{
  FunctionName: aws.String(functionName),
 })
 if err != nil {
  log.Panicf("Couldn't delete function %v. Here's why: %v\n", functionName, err)
 }
}
```

- Pour plus de détails sur l'API, voir DeleteFunction dans AWS SDK pour Go Référence d'API.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
   /**
    * Deletes an AWS Lambda function.
    *
    * @param awsLambda     an instance of the {@link LambdaClient} class, which
is used to interact with the AWS Lambda service
    * @param functionName  the name of the Lambda function to be deleted
    *
    * @throws LambdaException if an error occurs while deleting the Lambda
function
    */
   public static void deleteLambdaFunction(LambdaClient awsLambda, String
functionName) {
       try {
           DeleteFunctionRequest request = DeleteFunctionRequest.builder()
               .functionName(functionName)
               .build();

           awsLambda.deleteFunction(request);
           System.out.println("The " + functionName + " function was deleted");

       } catch (LambdaException e) {
           System.err.println(e.getMessage());
           System.exit(1);
       }
   }
```

- Pour plus de détails sur l'API, voir DeleteFunction dans AWS SDK for Java 2.x Référence d'API.

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
/**
 * @param {string} funcName
 */
const deleteFunction = (funcName) => {
  const client = new LambdaClient({});
  const command = new DeleteFunctionCommand({ FunctionName: funcName });
  return client.send(command);
};
```

- Pour plus de détails sur l'API, voir DeleteFunction dans AWS SDK pour JavaScript Référence d'API.

Kotlin

SDK pour Kotlin

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
suspend fun delLambdaFunction(myFunctionName: String) {
    val request =
```

```
        DeleteFunctionRequest {
            functionName = myFunctionName
        }

    LambdaClient { region = "us-east-1" }.use { awsLambda ->
        awsLambda.deleteFunction(request)
        println("$myFunctionName was deleted")
    }
}
```

- Pour plus de détails sur l'API, voir DeleteFunction dans AWS Référence du SDK pour l'API Kotlin.

PHP

Kit SDK pour PHP

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    public function deleteFunction($functionName)
    {
        return $this->lambdaClient->deleteFunction([
            'FunctionName' => $functionName,
        ]);
    }
```

- Pour plus de détails sur l'API, voir DeleteFunction dans AWS SDK pour PHP Référence d'API.

PowerShell

Outils pour PowerShell V4

Exemple 1 : cet exemple supprime une version spécifique d'une fonction Lambda

```
Remove-LMFunction -FunctionName "MylambdaFunction123" -Qualifier '3'
```

- Pour plus de détails sur l'API, voir DeleteFunction dans Outils AWS pour PowerShell Référence de l'applet de commande (V4).

Outils pour PowerShell V5

Exemple 1 : cet exemple supprime une version spécifique d’une fonction Lambda

```
Remove-LMFunction -FunctionName "MylambdaFunction123" -Qualifier '3'
```

- Pour plus de détails sur l'API, voir DeleteFunction dans Outils AWS pour PowerShell Référence de l'applet de commande (V5).

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l’exemple complet et découvrez comment le configurer et l’exécuter dans le référentiel d’exemples de code AWS.

```
class LambdaWrapper:
    def __init__(self, lambda_client, iam_resource):
        self.lambda_client = lambda_client
        self.iam_resource = iam_resource


    def delete_function(self, function_name):
        """
        Deletes a Lambda function.

        :param function_name: The name of the function to delete.
        """
        try:
            self.lambda_client.delete_function(FunctionName=function_name)
        except ClientError:
            logger.exception("Couldn't delete function %s.", function_name)
```

```
            raise
```

- Pour plus de détails sur l'API, voir DeleteFunction dans AWS Référence de l'API du SDK pour Python (Boto3).

Ruby

Kit SDK pour Ruby

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class LambdaWrapper
  attr_accessor :lambda_client, :cloudwatch_client, :iam_client

  def initialize
    @lambda_client = Aws::Lambda::Client.new
    @cloudwatch_client = Aws::CloudWatchLogs::Client.new(region: 'us-east-1')
    @iam_client = Aws::IAM::Client.new(region: 'us-east-1')
    @logger = Logger.new($stdout)
    @logger.level = Logger::WARN
  end

  # Deletes a Lambda function.
  # @param function_name: The name of the function to delete.
  def delete_function(function_name)
    print "Deleting function: #{function_name}..."
    @lambda_client.delete_function(
      function_name: function_name
    )
    print 'Done!'.green
  rescue Aws::Lambda::Errors::ServiceException => e
    @logger.error("There was an error deleting #{function_name}:\n #{e.message}")
  end
```

- Pour plus de détails sur l'API, voir DeleteFunction dans AWS SDK pour Ruby Référence d'API.

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
   /** Delete a function and its role, and if possible or necessary, its
associated code object and bucket. */
   pub async fn delete_function(
       &self,
       location: Option<String>,
   ) -> (
       Result<DeleteFunctionOutput, anyhow::Error>,
       Result<DeleteRoleOutput, anyhow::Error>,
       Option<Result<DeleteObjectOutput, anyhow::Error>>,
   ) {
       info!("Deleting lambda function {}", self.lambda_name);
       let delete_function = self
           .lambda_client
           .delete_function()
           .function_name(self.lambda_name.clone())
           .send()
           .await
           .map_err(anyhow::Error::from);

       info!("Deleting iam role {}", self.role_name);
       let delete_role = self
           .iam_client
           .delete_role()
           .role_name(self.role_name.clone())
           .send()
           .await
           .map_err(anyhow::Error::from);
```

```
        let delete_object: Option<Result<DeleteObjectOutput, anyhow::Error>> =
            if let Some(location) = location {
                info!("Deleting object {location}");
                Some(
                    self.s3_client
                        .delete_object()
                        .bucket(self.bucket.clone())
                        .key(location)
                        .send()
                        .await
                        .map_err(anyhow::Error::from),
                )
            } else {
                info!(?location, "Skipping delete object");
                None
            };

        (delete_function, delete_role, delete_object)
    }
```

- Pour plus de détails sur l'API, voir DeleteFunction dans AWS Référence de l'API SDK pour Rust.

SAP ABAP

Kit SDK pour SAP ABAP

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    TRY.
        lo_lmd->deletefunction( iv_functionname = iv_function_name ).
        MESSAGE 'Lambda function deleted.' TYPE 'I'.
      CATCH /aws1/cx_lmdinvparamvalueex.
        MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
      CATCH /aws1/cx_lmdresourceconflictex.
```

```
        MESSAGE 'Resource already exists or another operation is in progress.'
 TYPE 'E'.
      CATCH /aws1/cx_lmdresourcenotfoundex.
        MESSAGE 'The requested resource does not exist.' TYPE 'E'.
      CATCH /aws1/cx_lmdserviceexception.
        MESSAGE 'An internal problem was encountered by the AWS Lambda service.'
 TYPE 'E'.
      CATCH /aws1/cx_lmdtoomanyrequestsex.
        MESSAGE 'The maximum request throughput was reached.' TYPE 'E'.
    ENDTRY.
```

- Pour plus de détails sur l'API, voir DeleteFunction dans AWS Référence du SDK pour l'API SAP ABAP.

Swift

Kit SDK pour Swift

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import AWSClientRuntime
import AWSLambda
import Foundation

        do {
            _ = try await lambdaClient.deleteFunction(
                input: DeleteFunctionInput(
                    functionName: "lambda-basics-function"
                )
            )
        } catch {
            print("Error: Unable to delete the function.")
        }
```

- Pour plus de détails sur l'API, voir DeleteFunction dans AWS Référence du SDK pour l'API Swift.

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Utilisation de **`DeleteFunctionConcurrency`** avec une CLI

Les exemples de code suivants illustrent comment utiliser `DeleteFunctionConcurrency`.

CLI

AWS CLI

Pour supprimer une limite d'exécution simultanée d'une fonction

L'exemple `delete-function-concurrency` suivant supprime la limite d'exécution simultanée réservée de la fonction `my-function`.

```
aws lambda delete-function-concurrency \
    --function-name  my-function
```

Cette commande ne produit aucune sortie.

Pour plus d'informations, consultez Réservation de simultanéité pour une fonction Lambda dans le Guide du développeur AWS Lambda.

- Pour plus de détails sur l'API, voir DeleteFunctionConcurrency dans AWS CLI Référence de commande.

PowerShell

Outils pour PowerShell V4

Exemple 1 : cet exemple supprime la simultanéité des fonctions de la fonction Lambda.

```
Remove-LMFunctionConcurrency -FunctionName "MylambdaFunction123"
```

- Pour plus de détails sur l'API, voir DeleteFunctionConcurrency dans Outils AWS pour PowerShell Référence de l'applet de commande (V4).

Outils pour PowerShell V5

Exemple 1 : cet exemple supprime la simultanéité des fonctions de la fonction Lambda.

```
Remove-LMFunctionConcurrency -FunctionName "MylambdaFunction123"
```

- Pour plus de détails sur l'API, voir DeleteFunctionConcurrency dans Outils AWS pour PowerShell Référence de l'applet de commande (V5).

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Utilisation de **`DeleteProvisionedConcurrencyConfig`** avec une CLI

Les exemples de code suivants illustrent comment utiliser `DeleteProvisionedConcurrencyConfig`.

CLI

AWS CLI

Pour supprimer une configuration de simultanéité allouée

L'exemple `delete-provisioned-concurrency-config` suivant supprime la configuration de simultanéité allouée pour l'alias `GREEN` de la fonction spécifiée.

```
aws lambda delete-provisioned-concurrency-config \
    --function-name my-function \
    --qualifier GREEN
```

Cette commande ne produit aucune sortie.

Pour plus d'informations, voir Configuration de la simultanéité provisionnée pour une fonction événementielle dans le AWS Guide du développeur Lambda.

- Pour plus de détails sur l'API, voir DeleteProvisionedConcurrencyConfig dans AWS CLI Référence de commande.

PowerShell

Outils pour PowerShell V4

Exemple 1 : cet exemple supprime la configuration de simultanéité allouée pour un alias spécifique.

```
Remove-LMProvisionedConcurrencyConfig -FunctionName "MylambdaFunction123" -
Qualifier "NewAlias1"
```

- Pour plus de détails sur l'API, voir DeleteProvisionedConcurrencyConfig dans Outils AWS pour PowerShell Référence de l'applet de commande (V4).

Outils pour PowerShell V5

Exemple 1 : cet exemple supprime la configuration de simultanéité allouée pour un alias spécifique.

```
Remove-LMProvisionedConcurrencyConfig -FunctionName "MylambdaFunction123" -
Qualifier "NewAlias1"
```

- Pour plus de détails sur l'API, voir DeleteProvisionedConcurrencyConfig dans Outils AWS pour PowerShell Référence de l'applet de commande (V5).

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Utilisation de **`GetAccountSettings`** avec une CLI

Les exemples de code suivants illustrent comment utiliser `GetAccountSettings`.

CLI

AWS CLI

Pour récupérer les informations relatives à votre compte dans AWS Région

L'exemple `get-account-settings` suivant affiche les limites Lambda et les informations d'utilisation de votre compte.

```
aws lambda get-account-settings
```

Sortie :

```
{
    "AccountLimit": {
        "CodeSizeUnzipped": 262144000,
        "UnreservedConcurrentExecutions": 1000,
        "ConcurrentExecutions": 1000,
        "CodeSizeZipped": 52428800,
        "TotalCodeSize": 80530636800
    },
    "AccountUsage": {
        "FunctionCount": 4,
        "TotalCodeSize": 9426
    }
}
```

Pour plus d'informations, consultez Limites AWS Lambda dans le Guide du développeur AWS Lambda.

- Pour plus de détails sur l'API, voir GetAccountSettings dans AWS CLI Référence de commande.

PowerShell

Outils pour PowerShell V4

Exemple 1 : cet exemple affiche une comparaison entre la limite et l'utilisation du compte

```
Get-LMAccountSetting | Select-Object
 @{Name="TotalCodeSizeLimit";Expression={$_.AccountLimit.TotalCodeSize}},
 @{Name="TotalCodeSizeUsed";Expression={$_.AccountUsage.TotalCodeSize}}
```

Sortie :

```
TotalCodeSizeLimit TotalCodeSizeUsed
------------------ -----------------
       80530636800          15078795
```

- Pour plus de détails sur l'API, voir GetAccountSettings dans Outils AWS pour PowerShell Référence de l'applet de commande (V4).

Outils pour PowerShell V5

Exemple 1 : cet exemple affiche une comparaison entre la limite et l'utilisation du compte

```
Get-LMAccountSetting | Select-Object
 @{Name="TotalCodeSizeLimit";Expression={$_.AccountLimit.TotalCodeSize}},
 @{Name="TotalCodeSizeUsed";Expression={$_.AccountUsage.TotalCodeSize}}
```

Sortie :

```
TotalCodeSizeLimit TotalCodeSizeUsed
------------------ -----------------
       80530636800          15078795
```

- Pour plus de détails sur l'API, voir GetAccountSettings dans Outils AWS pour PowerShell Référence de l'applet de commande (V5).

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Utilisation de **`GetAlias`** avec une CLI

Les exemples de code suivants illustrent comment utiliser `GetAlias`.

CLI

AWS CLI

Pour récupérer les informations relatives à un alias de fonction

L'exemple `get-alias` suivant affiche les détails de l'alias nommé `LIVE` de la fonction Lambda `my-function`.

```
aws lambda get-alias \
    --function-name my-function \
    --name LIVE
```

Sortie :

```
{
    "FunctionVersion": "3",
    "Name": "LIVE",
    "AliasArn": "arn:aws:lambda:us-west-2:123456789012:function:my-
function:LIVE",
    "RevisionId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Description": "alias for live version of function"
}
```

Pour plus d'informations, voir Configuration AWS Alias de fonctions Lambda dans le AWS Guide du développeur Lambda.

- Pour plus de détails sur l'API, voir GetAlias dans AWS CLI Référence de commande.

PowerShell

Outils pour PowerShell V4

Exemple 1 : cet exemple récupère les poids de la configuration de routage pour un alias de fonction Lambda spécifique.

```
Get-LMAlias -FunctionName "MylambdaFunction123" -Name "newlabel1" -Select
 RoutingConfig
```

Sortie :

```
AdditionalVersionWeights
------------------------
{[1, 0.6]}
```

- Pour plus de détails sur l'API, voir GetAlias dans Outils AWS pour PowerShell Référence de l'applet de commande (V4).

Outils pour PowerShell V5

Exemple 1 : cet exemple récupère les poids de la configuration de routage pour un alias de fonction Lambda spécifique.

```
Get-LMAlias -FunctionName "MylambdaFunction123" -Name "newlabel1" -Select
 RoutingConfig
```

Sortie :

```
AdditionalVersionWeights
------------------------
{[1, 0.6]}
```

- Pour plus de détails sur l'API, voir GetAlias dans Outils AWS pour PowerShell Référence de l'applet de commande (V5).

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Utiliser **`GetFunction`** avec un AWS SDK ou CLI

Les exemples de code suivants illustrent comment utiliser `GetFunction`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans les exemples de code suivants :

- Principes de base
- Création de votre première fonction sans serveur

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    /// <summary>
    /// Gets information about a Lambda function.
    /// </summary>
    /// <param name="functionName">The name of the Lambda function for
    /// which to retrieve information.</param>
```

```
    /// <returns>Async Task.</returns>
    public async Task<FunctionConfiguration> GetFunctionAsync(string
functionName)
    {
        var functionRequest = new GetFunctionRequest
        {
            FunctionName = functionName,
        };

        var response = await _lambdaService.GetFunctionAsync(functionRequest);
        return response.Configuration;
    }
```

- Pour plus de détails sur l'API, voir GetFunction dans AWS SDK pour .NET Référence d'API.

C++

SDK pour C++

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
        Aws::Client::ClientConfiguration clientConfig;
        // Optional: Set to the AWS Region in which the bucket was created
(overrides config file).
        // clientConfig.region = "us-east-1";

    Aws::Lambda::LambdaClient client(clientConfig);

        Aws::Lambda::Model::GetFunctionRequest request;
        request.SetFunctionName(functionName);

        Aws::Lambda::Model::GetFunctionOutcome outcome =
client.GetFunction(request);

        if (outcome.IsSuccess()) {
            std::cout << "Function retrieve.\n" <<
```

```
 outcome.GetResult().GetConfiguration().Jsonize().View().WriteReadable()
                     << std::endl;
        }
        else {
            std::cerr << "Error with Lambda::GetFunction. "
                      << outcome.GetError().GetMessage()
                      << std::endl;
        }
```

- Pour plus de détails sur l'API, voir GetFunction dans AWS SDK pour C++ Référence d'API.

CLI

AWS CLI

Pour récupérer les informations sur une fonction

L'exemple `get-function` suivant affiche des informations sur la fonction `my-function`.

```
aws lambda get-function \
    --function-name  my-function
```

Sortie :

```
{
    "Concurrency": {
        "ReservedConcurrentExecutions": 100
    },
    "Code": {
        "RepositoryType": "S3",
        "Location": "https://awslambda-us-west-2-tasks.s3.us-
west-2.amazonaws.com/snapshots/123456789012/my-function..."
    },
    "Configuration": {
        "TracingConfig": {
            "Mode": "PassThrough"
        },
        "Version": "$LATEST",
        "CodeSha256": "5tT2qgzYUHoqwR616pZ2dpkn/0J1FrzJmlKidWaaCgk=",
        "FunctionName": "my-function",
        "VpcConfig": {
```

```
            "SubnetIds": [],
            "VpcId": "",
            "SecurityGroupIds": []
        },
        "MemorySize": 128,
        "RevisionId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "CodeSize": 304,
        "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-
function",
        "Handler": "index.handler",
        "Role": "arn:aws:iam::123456789012:role/service-role/helloWorldPython-
role-uy3l9qyq",
        "Timeout": 3,
        "LastModified": "2025-09-24T18:20:35.054+0000",
        "Runtime": "nodejs22.x",
        "Description": ""
    }
}
```

Pour plus d'informations, consultez Configurer la mémoire de fonction Lambda dans le Guide du développeur AWS Lambda.

- Pour plus de détails sur l'API, voir GetFunction dans AWS CLI Référence de commande.

Go

Kit SDK pour Go V2

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import (
 "bytes"
 "context"
 "encoding/json"
 "errors"
 "log"
 "time"
```

```
 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/service/lambda"
 "github.com/aws/aws-sdk-go-v2/service/lambda/types"
)

// FunctionWrapper encapsulates function actions used in the examples.
// It contains an AWS Lambda service client that is used to perform user actions.
type FunctionWrapper struct {
 LambdaClient *lambda.Client
}



// GetFunction gets data about the Lambda function specified by functionName.
func (wrapper FunctionWrapper) GetFunction(ctx context.Context, functionName
 string) types.State {
 var state types.State
 funcOutput, err := wrapper.LambdaClient.GetFunction(ctx,
 &lambda.GetFunctionInput{
  FunctionName: aws.String(functionName),
 })
 if err != nil {
  log.Panicf("Couldn't get function %v. Here's why: %v\n", functionName, err)
 } else {
  state = funcOutput.Configuration.State
 }
 return state
}
```

- Pour plus de détails sur l'API, voir GetFunction dans AWS SDK pour Go Référence d'API.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    /**
     * Retrieves information about an AWS Lambda function.
     *
     * @param awsLambda    an instance of the {@link LambdaClient} class, which
is used to interact with the AWS Lambda service
     * @param functionName the name of the AWS Lambda function to retrieve
information about
     */
    public static void getFunction(LambdaClient awsLambda, String functionName) {
        try {
            GetFunctionRequest functionRequest = GetFunctionRequest.builder()
                .functionName(functionName)
                .build();

            GetFunctionResponse response =
awsLambda.getFunction(functionRequest);
            System.out.println("The runtime of this Lambda function is " +
response.configuration().runtime());

        } catch (LambdaException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
```

- Pour plus de détails sur l'API, voir GetFunction dans AWS SDK for Java 2.x Référence d'API.

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
const getFunction = (funcName) => {
  const client = new LambdaClient({});
```

```
  const command = new GetFunctionCommand({ FunctionName: funcName });
  return client.send(command);
};
```

- Pour plus de détails sur l'API, voir GetFunction dans AWS SDK pour JavaScript Référence d'API.

PHP

Kit SDK pour PHP

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    public function getFunction($functionName)
    {
        return $this->lambdaClient->getFunction([
            'FunctionName' => $functionName,
        ]);
    }
```

- Pour plus de détails sur l'API, voir GetFunction dans AWS SDK pour PHP Référence d'API.

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class LambdaWrapper:
```

```
    def __init__(self, lambda_client, iam_resource):
        self.lambda_client = lambda_client
        self.iam_resource = iam_resource


    def get_function(self, function_name):
        """
        Gets data about a Lambda function.

        :param function_name: The name of the function.
        :return: The function data.
        """
        response = None
        try:
            response =
self.lambda_client.get_function(FunctionName=function_name)
        except ClientError as err:
            if err.response["Error"]["Code"] == "ResourceNotFoundException":
                logger.info("Function %s does not exist.", function_name)
            else:
                logger.error(
                    "Couldn't get function %s. Here's why: %s: %s",
                    function_name,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        return response
```

- Pour plus de détails sur l'API, voir GetFunction dans AWS Référence de l'API du SDK pour Python (Boto3).

Ruby

Kit SDK pour Ruby

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class LambdaWrapper
  attr_accessor :lambda_client, :cloudwatch_client, :iam_client

  def initialize
    @lambda_client = Aws::Lambda::Client.new
    @cloudwatch_client = Aws::CloudWatchLogs::Client.new(region: 'us-east-1')
    @iam_client = Aws::IAM::Client.new(region: 'us-east-1')
    @logger = Logger.new($stdout)
    @logger.level = Logger::WARN
  end

  # Gets data about a Lambda function.
  #
  # @param function_name: The name of the function.
  # @return response: The function data, or nil if no such function exists.
  def get_function(function_name)
    @lambda_client.get_function(
      {
        function_name: function_name
      }
    )
  rescue Aws::Lambda::Errors::ResourceNotFoundException => e
    @logger.debug("Could not find function: #{function_name}:\n #{e.message}")
    nil
  end
```

- Pour plus de détails sur l'API, voir GetFunction dans AWS SDK pour Ruby Référence d'API.

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
   /** Get the Lambda function with this Manager's name. */
   pub async fn get_function(&self) -> Result<GetFunctionOutput, anyhow::Error>
{
       info!("Getting lambda function");
       self.lambda_client
           .get_function()
           .function_name(self.lambda_name.clone())
           .send()
           .await
           .map_err(anyhow::Error::from)
   }
```

- Pour plus de détails sur l'API, voir GetFunction dans AWS Référence de l'API SDK pour Rust.

SAP ABAP

Kit SDK pour SAP ABAP

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
   TRY.
       oo_result = lo_lmd->getfunction( iv_functionname = iv_function_name ).
" oo_result is returned for testing purposes. "
```

```
        MESSAGE 'Lambda function information retrieved.' TYPE 'I'.
      CATCH /aws1/cx_lmdinvparamvalueex.
        MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
      CATCH /aws1/cx_lmdserviceexception.
        MESSAGE 'An internal problem was encountered by the AWS Lambda service.'
 TYPE 'E'.
      CATCH /aws1/cx_lmdtoomanyrequestsex.
        MESSAGE 'The maximum request throughput was reached.' TYPE 'E'.
    ENDTRY.
```

- Pour plus de détails sur l'API, voir GetFunction dans AWS Référence du SDK pour l'API SAP ABAP.

Swift

Kit SDK pour Swift

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import AWSClientRuntime
import AWSLambda
import Foundation

    /// Detect whether or not the AWS Lambda function with the specified name
    /// exists, by requesting its function information.
    ///
    /// - Parameters:
    ///   - lambdaClient: The `LambdaClient` to use.
    ///   - name: The name of the AWS Lambda function to find.
    ///
    /// - Returns: `true` if the Lambda function exists. Otherwise `false`.
    func doesLambdaFunctionExist(lambdaClient: LambdaClient, name: String) async
 -> Bool {
        do {
            _ = try await lambdaClient.getFunction(
                input: GetFunctionInput(functionName: name)
```

```
            )
        } catch {
            return false
        }

        return true
    }
```

- Pour plus de détails sur l'API, voir GetFunction dans AWS Référence du SDK pour l'API Swift.

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Utilisation de **`GetFunctionConcurrency`** avec une CLI

Les exemples de code suivants illustrent comment utiliser `GetFunctionConcurrency`.

CLI

AWS CLI

Pour afficher le paramètre de simultanéité réservé pour une fonction

L'exemple `get-function-concurrency` suivant récupère le paramètre de simultanéité réservé pour la fonction spécifiée.

```
aws lambda get-function-concurrency \
    --function-name my-function
```

Sortie :

```
{
    "ReservedConcurrentExecutions": 250
}
```

Pour plus d'informations, voir Configuration de la simultanéité réservée pour une fonction événementielle dans le AWS Guide du développeur Lambda.

- Pour plus de détails sur l'API, voir GetFunctionConcurrency dans AWS CLI Référence de commande.

PowerShell

Outils pour PowerShell V4

Exemple 1 : cet exemple permet d'obtenir la simultanéité réservée pour la fonction Lambda

```
Get-LMFunctionConcurrency -FunctionName "MylambdaFunction123" -Select *
```

Sortie :

```
ReservedConcurrentExecutions
----------------------------
100
```

- Pour plus de détails sur l'API, voir GetFunctionConcurrency dans Outils AWS pour PowerShell Référence de l'applet de commande (V4).

Outils pour PowerShell V5

Exemple 1 : cet exemple permet d'obtenir la simultanéité réservée pour la fonction Lambda

```
Get-LMFunctionConcurrency -FunctionName "MylambdaFunction123" -Select *
```

Sortie :

```
ReservedConcurrentExecutions
----------------------------
100
```

- Pour plus de détails sur l'API, voir GetFunctionConcurrency dans Outils AWS pour PowerShell Référence de l'applet de commande (V5).

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Utilisation de **`GetFunctionConfiguration`** avec une CLI

Les exemples de code suivants illustrent comment utiliser `GetFunctionConfiguration`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l'exemple de code suivant :

- Création de votre première fonction sans serveur

CLI

AWS CLI

Pour récupérer les paramètres d'une fonction Lambda spécifiques à sa version

L'exemple `get-function-configuration` suivant affiche les paramètres de la version 2 de la fonction `my-function`.

```
aws lambda get-function-configuration \
    --function-name  my-function:2
```

Sortie :

```
{
    "FunctionName": "my-function",
    "LastModified": "2019-09-26T20:28:40.438+0000",
    "RevisionId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "MemorySize": 256,
    "Version": "2",
    "Role": "arn:aws:iam::123456789012:role/service-role/my-function-role-
uy3l9qyq",
    "Timeout": 3,
    "Runtime": "nodejs10.x",
    "TracingConfig": {
        "Mode": "PassThrough"
    },
    "CodeSha256": "5tT2qgzYUHaqwR716pZ2dpkn/0J1FrzJmlKidWoaCgk=",
    "Description": "",
    "VpcConfig": {
        "SubnetIds": [],
```

```
        "VpcId": "",
        "SecurityGroupIds": []
    },
    "CodeSize": 304,
    "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-
function:2",
    "Handler": "index.handler"
}
```

Pour plus d'informations, consultez Configuration des options de fonction Lambda AWS dans le Guide du développeur AWS .

- Pour plus de détails sur l'API, voir GetFunctionConfiguration dans AWS CLI Référence de commande.

PowerShell

Outils pour PowerShell V4

Exemple 1 : cet exemple renvoie la configuration spécifique à la version d'une fonction Lambda.

```
Get-LMFunctionConfiguration -FunctionName "MylambdaFunction123" -Qualifier
 "PowershellAlias"
```

Sortie :

```
CodeSha256                  : uWOW0R7z+f0VyLuUg7+/D08hkMFsq0SF4seuyUZJ/R8=
CodeSize                    : 1426
DeadLetterConfig            : Amazon.Lambda.Model.DeadLetterConfig
Description                 : Verson 3 to test Aliases
Environment                 : Amazon.Lambda.Model.EnvironmentResponse
FunctionArn                 : arn:aws:lambda:us-
east-1:123456789012:function:MylambdaFunction123
                              :PowershellAlias
FunctionName                : MylambdaFunction123
Handler                     : lambda_function.launch_instance
KMSKeyArn                   :
LastModified                : 2019-12-25T09:52:59.872+0000
LastUpdateStatus            : Successful
LastUpdateStatusReason      :
LastUpdateStatusReasonCode  :
```

```
Layers                       : {}
MasterArn                    :
MemorySize                   : 128
RevisionId                   : 5d7de38b-87f2-4260-8f8a-e87280e10c33
Role                         : arn:aws:iam::123456789012:role/service-role/lambda
Runtime                      : python3.8
State                        : Active
StateReason                  :
StateReasonCode              :
Timeout                      : 600
TracingConfig                : Amazon.Lambda.Model.TracingConfigResponse
Version                      : 4
VpcConfig                    : Amazon.Lambda.Model.VpcConfigDetail
```

- Pour plus de détails sur l'API, voir GetFunctionConfiguration dans Outils AWS pour PowerShell Référence de l'applet de commande (V4).

Outils pour PowerShell V5

Exemple 1 : cet exemple renvoie la configuration spécifique à la version d'une fonction Lambda.

```
Get-LMFunctionConfiguration -FunctionName "MylambdaFunction123" -Qualifier
 "PowershellAlias"
```

Sortie :

```
CodeSha256                   : uWOW0R7z+f0VyLuUg7+/D08hkMFsq0SF4seuyUZJ/R8=
CodeSize                     : 1426
DeadLetterConfig             : Amazon.Lambda.Model.DeadLetterConfig
Description                  : Verson 3 to test Aliases
Environment                  : Amazon.Lambda.Model.EnvironmentResponse
FunctionArn                  : arn:aws:lambda:us-
east-1:123456789012:function:MylambdaFunction123
                               :PowershellAlias
FunctionName                 : MylambdaFunction123
Handler                      : lambda_function.launch_instance
KMSKeyArn                    :
LastModified                 : 2019-12-25T09:52:59.872+0000
LastUpdateStatus             : Successful
LastUpdateStatusReason       :
LastUpdateStatusReasonCode   :
Layers                       : {}
```

```
MasterArn                 :
MemorySize                : 128
RevisionId                : 5d7de38b-87f2-4260-8f8a-e87280e10c33
Role                      : arn:aws:iam::123456789012:role/service-role/lambda
Runtime                   : python3.8
State                     : Active
StateReason               :
StateReasonCode           :
Timeout                   : 600
TracingConfig             : Amazon.Lambda.Model.TracingConfigResponse
Version                   : 4
VpcConfig                 : Amazon.Lambda.Model.VpcConfigDetail
```

- Pour plus de détails sur l'API, voir GetFunctionConfiguration dans Outils AWS pour PowerShell Référence de l'applet de commande (V5).

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Utilisation de **`GetPolicy`** avec une CLI

Les exemples de code suivants illustrent comment utiliser `GetPolicy`.

CLI

AWS CLI

Pour récupérer la politique IAM basée sur les ressources d'une fonction, d'une version ou d'un alias

L'exemple `get-policy` suivant affiche les informations de politique relative à la fonction Lambda `my-function`.

```
aws lambda get-policy \
    --function-name my-function
```

Sortie :

```
{
```

```
    "Policy": "{\"Version\":\"2012-10-17\",\"Id\":\"default\",\"Statement
\":[{\"Sid\":\"iot-events\",\"Effect\":\"Allow\",\"Principal\":{\"Service\":
\"iotevents.amazonaws.com\"},\"Action\":\"lambda:InvokeFunction\",\"Resource\":
\"arn:aws:lambda:us-west-2:123456789012:function:my-function\"}]}",
    "RevisionId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

Pour plus d'informations, voir En utilisant Resource-based Politiques pour AWS Lambda dans le AWS Guide du développeur Lambda.

- Pour plus de détails sur l'API, voir GetPolicy dans AWS CLI Référence de commande.

PowerShell

Outils pour PowerShell V4

Exemple 1 : cet exemple affiche la stratégie de fonction de la fonction Lambda

```
Get-LMPolicy -FunctionName test -Select Policy
```

Sortie :

```
{"Version":"2012-10-17",       "Id":"default","Statement":
[{"Sid":"xxxx","Effect":"Allow","Principal":
{"Service":"sns.amazonaws.com"},"Action":"lambda:InvokeFunction","Resource":"arn:aws:lamb
east-1:123456789102:function:test"}]}
```

- Pour plus de détails sur l'API, voir GetPolicy dans Outils AWS pour PowerShell Référence de l'applet de commande (V4).

Outils pour PowerShell V5

Exemple 1 : cet exemple affiche la stratégie de fonction de la fonction Lambda

```
Get-LMPolicy -FunctionName test -Select Policy
```

Sortie :

```
{"Version":"2012-10-17",       "Id":"default","Statement":
[{"Sid":"xxxx","Effect":"Allow","Principal":
```

```
{"Service":"sns.amazonaws.com"},"Action":"lambda:InvokeFunction","Resource":"arn:aws:lamb
east-1:123456789102:function:test"}]}
```

- Pour plus de détails sur l'API, voir GetPolicy dans Outils AWS pour PowerShell Référence de l'applet de commande (V5).

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Utilisation de **`GetProvisionedConcurrencyConfig`** avec une CLI

Les exemples de code suivants illustrent comment utiliser `GetProvisionedConcurrencyConfig`.

CLI

AWS CLI

Pour afficher la configuration de la simultanéité allouée

L'exemple `get-provisioned-concurrency-config` suivant affiche les détails de la configuration de simultanéité allouée pour l'alias `BLUE` de la fonction spécifiée.

```
aws lambda get-provisioned-concurrency-config \
    --function-name my-function \
    --qualifier BLUE
```

Sortie :

```
{
    "RequestedProvisionedConcurrentExecutions": 100,
    "AvailableProvisionedConcurrentExecutions": 100,
    "AllocatedProvisionedConcurrentExecutions": 100,
    "Status": "READY",
    "LastModified": "2019-12-31T20:28:49+0000"
}
```

Pour plus d'informations, voir Configuration de la simultanéité provisionnée pour une fonction événementielle dans le AWS Guide du développeur Lambda.

- Pour plus de détails sur l'API, voir GetProvisionedConcurrencyConfig dans AWS CLI Référence de commande.

PowerShell

Outils pour PowerShell V4

Exemple 1 : cet exemple obtient la configuration de simultanéité allouée pour l'alias spécifié de la fonction Lambda.

```
C:\>Get-LMProvisionedConcurrencyConfig -FunctionName "MylambdaFunction123" -
Qualifier "NewAlias1"
```

Sortie :

```
AllocatedProvisionedConcurrentExecutions : 0
AvailableProvisionedConcurrentExecutions : 0
LastModified                             : 2020-01-15T03:21:26+0000
RequestedProvisionedConcurrentExecutions : 70
Status                                   : IN_PROGRESS
StatusReason                             :
```

- Pour plus de détails sur l'API, voir GetProvisionedConcurrencyConfig dans Outils AWS pour PowerShell Référence de l'applet de commande (V4).

Outils pour PowerShell V5

Exemple 1 : cet exemple obtient la configuration de simultanéité allouée pour l'alias spécifié de la fonction Lambda.

```
C:\>Get-LMProvisionedConcurrencyConfig -FunctionName "MylambdaFunction123" -
Qualifier "NewAlias1"
```

Sortie :

```
AllocatedProvisionedConcurrentExecutions : 0
AvailableProvisionedConcurrentExecutions : 0
LastModified                             : 2020-01-15T03:21:26+0000
RequestedProvisionedConcurrentExecutions : 70
Status                                   : IN_PROGRESS
StatusReason                             :
```

- Pour plus de détails sur l'API, voir GetProvisionedConcurrencyConfig dans Outils AWS pour PowerShell Référence de l'applet de commande (V5).

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Utiliser **`Invoquer`** avec un AWS SDK ou CLI

Les exemples de code suivants illustrent comment utiliser `Invoke`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans les exemples de code suivants :

- Principes de base
- Création d'un tableau de bord de surveillance avec le nom de fonction comme variable
- Création de votre première fonction sans serveur
- Utilisation de variables de propriété dans les tableaux de bord de surveillance pour surveiller plusieurs fonctions sans serveur

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    /// <summary>
    /// Invoke a Lambda function.
    /// </summary>
    /// <param name="functionName">The name of the Lambda function to
    /// invoke.</param
    /// <param name="parameters">The parameter values that will be passed to the
function.</param>
    /// <returns>A System Threading Task.</returns>
    public async Task<string> InvokeFunctionAsync(
        string functionName,
        string parameters)
    {
```

```
        var payload = parameters;
        var request = new InvokeRequest
        {
            FunctionName = functionName,
            Payload = payload,
        };

        var response = await _lambdaService.InvokeAsync(request);
        MemoryStream stream = response.Payload;
        string returnValue =
System.Text.Encoding.UTF8.GetString(stream.ToArray());
        return returnValue;
    }
```

- Pour en savoir plus sur l'API, consultez Invoke dans la Référence de l'API AWS SDK pour .NET .

C++

SDK pour C++

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
        Aws::Client::ClientConfiguration clientConfig;
        // Optional: Set to the AWS Region in which the bucket was created
(overrides config file).
        // clientConfig.region = "us-east-1";

    Aws::Lambda::LambdaClient client(clientConfig);

        Aws::Lambda::Model::InvokeRequest request;
        request.SetFunctionName(LAMBDA_NAME);
        request.SetLogType(logType);
        std::shared_ptr<Aws::IOStream> payload =
Aws::MakeShared<Aws::StringStream>(
```

```
            "FunctionTest");
        *payload << jsonPayload.View().WriteReadable();
        request.SetBody(payload);
        request.SetContentType("application/json");
        Aws::Lambda::Model::InvokeOutcome outcome = client.Invoke(request);

        if (outcome.IsSuccess()) {
            invokeResult = std::move(outcome.GetResult());
            result = true;
            break;
        }

        else {
            std::cerr << "Error with Lambda::InvokeRequest. "
                      << outcome.GetError().GetMessage()
                      << std::endl;
            break;
        }
```

- Pour en savoir plus sur l'API, consultez Invoke dans la Référence de l'API AWS SDK pour C++ .

CLI

AWS CLI

Exemple 1 : pour invoquer une fonction Lambda de manière synchrone

L'exemple `invoke` suivant invoque la fonction `my-function` de manière synchrone. Le `cli-binary-format` l'option est requise si vous utilisez AWS Version 2 de la CLI. Pour plus d'informations, veuillez consulter les options de ligne de commande prises en charge par la CLI AWS dans le Guide de l'interface de ligne de commande AWS .

```
aws lambda invoke response.json \
    --function-name my-function \
    --cli-binary-format raw-in-base64-out \
    --payload '{ "name": "Bob" }'
```

Sortie :

```
{
```

```
    "ExecutedVersion": "$LATEST",
    "StatusCode": 200
}
```

Pour plus d'informations, consultez Invocation d'une fonction Lambda de manière synchrone dans le Guide du développeur AWS Lambda.

Exemple 2 : pour invoquer une fonction Lambda de manière asynchrone

L'exemple `invoke` suivant invoque la fonction `my-function` de manière asynchrone. Le `cli-binary-format` l'option est requise si vous utilisez AWS Version 2 de la CLI. Pour plus d'informations, veuillez consulter les options de ligne de commande prises en charge par la CLI AWS dans le Guide de l'interface de ligne de commande AWS .

```
aws lambda invoke response.json \
    --function-name my-function \
    --invocation-type Event \
    --cli-binary-format raw-in-base64-out \
    --payload '{ "name": "Bob" }'
```

Sortie :

```
{
    "StatusCode": 202
}
```

Pour plus d'informations, consultez Invocation d'une fonction Lambda de manière asynchrone dans le Guide du développeur AWS Lambda.

- Pour plus d'informations sur l'API, consultez Invoke dans la Référence des commandes AWS CLI .

Go

Kit SDK pour Go V2

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import (
 "bytes"
 "context"
 "encoding/json"
 "errors"
 "log"
 "time"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/service/lambda"
 "github.com/aws/aws-sdk-go-v2/service/lambda/types"
)

// FunctionWrapper encapsulates function actions used in the examples.
// It contains an AWS Lambda service client that is used to perform user actions.
type FunctionWrapper struct {
 LambdaClient *lambda.Client
}



// Invoke invokes the Lambda function specified by functionName, passing the
 parameters
// as a JSON payload. When getLog is true, types.LogTypeTail is specified, which
 tells
// Lambda to include the last few log lines in the returned result.
func (wrapper FunctionWrapper) Invoke(ctx context.Context, functionName string,
 parameters any, getLog bool) *lambda.InvokeOutput {
 logType := types.LogTypeNone
 if getLog {
  logType = types.LogTypeTail
 }
 payload, err := json.Marshal(parameters)
 if err != nil {
  log.Panicf("Couldn't marshal parameters to JSON. Here's why %v\n", err)
 }
 invokeOutput, err := wrapper.LambdaClient.Invoke(ctx, &lambda.InvokeInput{
  FunctionName: aws.String(functionName),
  LogType:      logType,
  Payload:      payload,
 })
 if err != nil {
```

```
  log.Panicf("Couldn't invoke function %v. Here's why: %v\n", functionName, err)
 }
 return invokeOutput
}
```

- Pour en savoir plus sur l'API, consultez Invoke dans la Référence de l'API AWS SDK pour Go .

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
   /**
    * Invokes a specific AWS Lambda function.
    *
    * @param awsLambda    an instance of {@link LambdaClient} to interact with
the AWS Lambda service
    * @param functionName the name of the AWS Lambda function to be invoked
    */
   public static void invokeFunction(LambdaClient awsLambda, String
functionName) {
       InvokeResponse res;
       try {
           // Need a SdkBytes instance for the payload.
           JSONObject jsonObj = new JSONObject();
           jsonObj.put("inputValue", "2000");
           String json = jsonObj.toString();
           SdkBytes payload = SdkBytes.fromUtf8String(json);

           InvokeRequest request = InvokeRequest.builder()
               .functionName(functionName)
               .payload(payload)
               .build();
```

```
            res = awsLambda.invoke(request);
            String value = res.payload().asUtf8String();
            System.out.println(value);

        } catch (LambdaException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
```

- Pour en savoir plus sur l'API, consultez Invoke dans la Référence de l'API AWS SDK for Java 2.x .

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
const invoke = async (funcName, payload) => {
  const client = new LambdaClient({});
  const command = new InvokeCommand({
    FunctionName: funcName,
    Payload: JSON.stringify(payload),
    LogType: LogType.Tail,
  });

  const { Payload, LogResult } = await client.send(command);
  const result = Buffer.from(Payload).toString();
  const logs = Buffer.from(LogResult, "base64").toString();
  return { logs, result };
};
```

- Pour plus d'informations sur l'API, consultez Invoke dans la AWS SDK pour JavaScript Référence d'API.

Kotlin

SDK pour Kotlin

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
suspend fun invokeFunction(functionNameVal: String) {
    val json = """{"inputValue":"1000"}"""
    val byteArray = json.trimIndent().encodeToByteArray()
    val request =
        InvokeRequest {
            functionName = functionNameVal
            logType = LogType.Tail
            payload = byteArray
        }

    LambdaClient { region = "us-west-2" }.use { awsLambda ->
        val res = awsLambda.invoke(request)
        println("${res.payload?.toString(Charsets.UTF_8)}")
        println("The log result is ${res.logResult}")
    }
}
```

- Pour plus d'informations sur l'API, consultez Invoke dans la AWS Référence d'API du kit SDK pour Kotlin.

PHP

Kit SDK pour PHP

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    public function invoke($functionName, $params, $logType = 'None')
    {
        return $this->lambdaClient->invoke([
            'FunctionName' => $functionName,
            'Payload' => json_encode($params),
            'LogType' => $logType,
        ]);
    }
```

- Pour en savoir plus sur l'API, consultez Invoke dans la Référence de l'API AWS SDK pour PHP .

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class LambdaWrapper:
    def __init__(self, lambda_client, iam_resource):
        self.lambda_client = lambda_client
        self.iam_resource = iam_resource


    def invoke_function(self, function_name, function_params, get_log=False):
```

```
        """
        Invokes a Lambda function.

        :param function_name: The name of the function to invoke.
        :param function_params: The parameters of the function as a dict. This
dict
                                is serialized to JSON before it is sent to
Lambda.
        :param get_log: When true, the last 4 KB of the execution log are
included in
                        the response.
        :return: The response from the function invocation.
        """
        try:
            response = self.lambda_client.invoke(
                FunctionName=function_name,
                Payload=json.dumps(function_params),
                LogType="Tail" if get_log else "None",
            )
            logger.info("Invoked function %s.", function_name)
        except ClientError:
            logger.exception("Couldn't invoke function %s.", function_name)
            raise
        return response
```

- Pour plus d'informations sur l'API, consultez Invoke dans la AWS Référence d'API du kit SDK pour Python (Boto3).

Ruby

Kit SDK pour Ruby

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class LambdaWrapper
```

```
  attr_accessor :lambda_client, :cloudwatch_client, :iam_client

  def initialize
    @lambda_client = Aws::Lambda::Client.new
    @cloudwatch_client = Aws::CloudWatchLogs::Client.new(region: 'us-east-1')
    @iam_client = Aws::IAM::Client.new(region: 'us-east-1')
    @logger = Logger.new($stdout)
    @logger.level = Logger::WARN
  end

  # Invokes a Lambda function.
  # @param function_name [String] The name of the function to invoke.
  # @param payload [nil] Payload containing runtime parameters.
  # @return [Object] The response from the function invocation.
  def invoke_function(function_name, payload = nil)
    params = { function_name: function_name }
    params[:payload] = payload unless payload.nil?
    @lambda_client.invoke(params)
  rescue Aws::Lambda::Errors::ServiceException => e
    @logger.error("There was an error executing #{function_name}:\n
#{e.message}")
  end
```

- Pour en savoir plus sur l'API, consultez Invoke dans la Référence de l'API AWS SDK pour Ruby .

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    /** Invoke the lambda function using calculator InvokeArgs. */
    pub async fn invoke(&self, args: InvokeArgs) -> Result<InvokeOutput,
anyhow::Error> {
        info!(?args, "Invoking {}", self.lambda_name);
```

```
        let payload = serde_json::to_string(&args)?;
        debug!(?payload, "Sending payload");
        self.lambda_client
            .invoke()
            .function_name(self.lambda_name.clone())
            .payload(Blob::new(payload))
            .send()
            .await
            .map_err(anyhow::Error::from)
    }

fn log_invoke_output(invoke: &InvokeOutput, message: &str) {
    if let Some(payload) = invoke.payload().cloned() {
        let payload = String::from_utf8(payload.into_inner());
        info!(?payload, message);
    } else {
        info!("Could not extract payload")
    }
    if let Some(logs) = invoke.log_result() {
        debug!(?logs, "Invoked function logs")
    } else {
        debug!("Invoked function had no logs")
    }
}
```

- Pour plus d'informations sur l'API, consultez Invoquer dans la Référence d'API du kit SDK AWS pour Rust.

SAP ABAP

Kit SDK pour SAP ABAP

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    TRY.
        DATA(lv_json) = /aws1/cl_rt_util=>string_to_xstring(
```

```
          `{`  &&
            `"action": "increment",`  &&
            `"number": 10` &&
          `}` ).
        oo_result = lo_lmd->invoke(                  " oo_result is returned for
testing purposes. "
                 iv_functionname = iv_function_name
                 iv_payload = lv_json ).
        MESSAGE 'Lambda function invoked.' TYPE 'I'.
      CATCH /aws1/cx_lmdinvparamvalueex.
        MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
      CATCH /aws1/cx_lmdinvrequestcontex.
        MESSAGE 'Unable to parse request body as JSON.' TYPE 'E'.
      CATCH /aws1/cx_lmdinvalidzipfileex.
        MESSAGE 'The deployment package could not be unzipped.' TYPE 'E'.
      CATCH /aws1/cx_lmdrequesttoolargeex.
        MESSAGE 'Invoke request body JSON input limit was exceeded by the request
payload.' TYPE 'E'.
      CATCH /aws1/cx_lmdresourceconflictex.
        MESSAGE 'Resource already exists or another operation is in progress.'
TYPE 'E'.
      CATCH /aws1/cx_lmdresourcenotfoundex.
        MESSAGE 'The requested resource does not exist.' TYPE 'E'.
      CATCH /aws1/cx_lmdserviceexception.
        MESSAGE 'An internal problem was encountered by the AWS Lambda service.'
TYPE 'E'.
      CATCH /aws1/cx_lmdtoomanyrequestsex.
        MESSAGE 'The maximum request throughput was reached.' TYPE 'E'.
      CATCH /aws1/cx_lmdunsuppedmediatyp00.
        MESSAGE 'Invoke request body does not have JSON as its content type.'
TYPE 'E'.
    ENDTRY.
```

- Pour plus de détails sur l'API, consultez Invoke dans la Référence des API du kit AWS SDK pour SAP ABAP.

Swift

Kit SDK pour Swift

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import AWSClientRuntime
import AWSLambda
import Foundation

    /// Invoke the Lambda function to increment a value.
    ///
    /// - Parameters:
    ///   - lambdaClient: The `IAMClient` to use.
    ///   - number: The number to increment.
    ///
    /// - Throws: `ExampleError.noAnswerReceived`, `ExampleError.invokeError`
    ///
    /// - Returns: An integer number containing the incremented value.
    func invokeIncrement(lambdaClient: LambdaClient, number: Int) async throws ->
 Int {
        do {
            let incRequest = IncrementRequest(action: "increment", number:
 number)
            let incData = try! JSONEncoder().encode(incRequest)

            // Invoke the lambda function.

            let invokeOutput = try await lambdaClient.invoke(
                input: InvokeInput(
                    functionName: "lambda-basics-function",
                    payload: incData
                )
            )

            let response = try! JSONDecoder().decode(Response.self,
 from:invokeOutput.payload!)
```

```
            guard let answer = response.answer else {
                throw ExampleError.noAnswerReceived
            }
            return answer

        } catch {
            throw ExampleError.invokeError
        }
    }
```

- Pour plus de détails sur l'API, consultez Invoke dans la Référence des API du kit AWS SDK pour Swift.

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Utiliser **`ListFunctions`** avec un AWS SDK ou CLI

Les exemples de code suivants illustrent comment utiliser `ListFunctions`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans les exemples de code suivants :

- Principes de base
- Création d'un tableau de bord de surveillance avec le nom de fonction comme variable

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    /// <summary>
```

```
    /// Get a list of Lambda functions.
    /// </summary>
    /// <returns>A list of FunctionConfiguration objects.</returns>
    public async Task<List<FunctionConfiguration>> ListFunctionsAsync()
    {
        var functionList = new List<FunctionConfiguration>();

        var functionPaginator =
            _lambdaService.Paginators.ListFunctions(new ListFunctionsRequest());
        await foreach (var function in functionPaginator.Functions)
        {
            functionList.Add(function);
        }

        return functionList;
    }
```

- Pour plus de détails sur l'API, voir ListFunctions dans AWS SDK pour .NET Référence d'API.

C++

SDK pour C++

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
       Aws::Client::ClientConfiguration clientConfig;
       // Optional: Set to the AWS Region in which the bucket was created
(overrides config file).
       // clientConfig.region = "us-east-1";

   Aws::Lambda::LambdaClient client(clientConfig);

   std::vector<Aws::String> functions;
   Aws::String marker;
```

```
   do {
       Aws::Lambda::Model::ListFunctionsRequest request;
       if (!marker.empty()) {
           request.SetMarker(marker);
       }

       Aws::Lambda::Model::ListFunctionsOutcome outcome = client.ListFunctions(
               request);

       if (outcome.IsSuccess()) {
           const Aws::Lambda::Model::ListFunctionsResult &result =
outcome.GetResult();
           std::cout << result.GetFunctions().size()
                     << " lambda functions were retrieved." << std::endl;

           for (const Aws::Lambda::Model::FunctionConfiguration
&functionConfiguration: result.GetFunctions()) {
               functions.push_back(functionConfiguration.GetFunctionName());
               std::cout << functions.size() << "  "
                         << functionConfiguration.GetDescription() << std::endl;
               std::cout << "   "
                         <<
Aws::Lambda::Model::RuntimeMapper::GetNameForRuntime(
                                 functionConfiguration.GetRuntime()) << ": "
                         << functionConfiguration.GetHandler()
                         << std::endl;
           }
           marker = result.GetNextMarker();
       }
       else {
           std::cerr << "Error with Lambda::ListFunctions. "
                     << outcome.GetError().GetMessage()
                     << std::endl;
       }
   } while (!marker.empty());
```

- Pour plus de détails sur l'API, voir ListFunctions dans AWS SDK pour C++ Référence d'API.

CLI

AWS CLI

Pour récupérer la liste des fonctions Lambda

L'exemple `list-functions` suivant affiche une liste de toutes les fonctions pour l'utilisateur actuel.

```
aws lambda list-functions
```

Sortie :

```
{
    "Functions": [
        {
            "TracingConfig": {
                "Mode": "PassThrough"
            },
            "Version": "$LATEST",
            "CodeSha256": "dBG9m8SGdmlEjw/JYXlhhvCrAv5TxvXsbL/RMr0fT/I=",
            "FunctionName": "helloworld",
            "MemorySize": 128,
            "RevisionId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "CodeSize": 294,
            "FunctionArn": "arn:aws:lambda:us-
west-2:123456789012:function:helloworld",
            "Handler": "helloworld.handler",
            "Role": "arn:aws:iam::123456789012:role/service-role/MyTestFunction-
role-zgur6bf4",
            "Timeout": 3,
            "LastModified": "2025-09-23T18:32:33.857+0000",
            "Runtime": "nodejs22.x",
            "Description": ""
        },
        {
            "TracingConfig": {
                "Mode": "PassThrough"
            },
            "Version": "$LATEST",
            "CodeSha256": "sU0cJ2/hOZevwV/lTxCuQqK3gDZP3i8gUoqUUVRmY6E=",
            "FunctionName": "my-function",
            "VpcConfig": {
```

```
                "SubnetIds": [],
                "VpcId": "",
                "SecurityGroupIds": []
            },
            "MemorySize": 256,
            "RevisionId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
            "CodeSize": 266,
            "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-
function",
            "Handler": "index.handler",
            "Role": "arn:aws:iam::123456789012:role/service-role/
helloWorldPython-role-uy3l9qyq",
            "Timeout": 3,
            "LastModified": "2025-10-01T16:47:28.490+0000",
            "Runtime": "nodejs22.x",
            "Description": ""
        },
        {
            "Layers": [
                {
                    "CodeSize": 41784542,
                    "Arn": "arn:aws:lambda:us-
west-2:420165488524:layer:AWSLambda-Python37-SciPy1x:2"
                },
                {
                    "CodeSize": 4121,
                    "Arn": "arn:aws:lambda:us-
west-2:123456789012:layer:pythonLayer:1"
                }
            ],
            "TracingConfig": {
                "Mode": "PassThrough"
            },
            "Version": "$LATEST",
            "CodeSha256": "ZQukCqxtkqFgyF2cU41Avj99TKQ/hNihPtDtRcc08mI=",
            "FunctionName": "my-python-function",
            "VpcConfig": {
                "SubnetIds": [],
                "VpcId": "",
                "SecurityGroupIds": []
            },
            "MemorySize": 128,
            "RevisionId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
            "CodeSize": 299,
```

```
            "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-
python-function",
            "Handler": "lambda_function.lambda_handler",
            "Role": "arn:aws:iam::123456789012:role/service-role/my-python-
function-role-z5g7dr6n",
            "Timeout": 3,
            "LastModified": "2025-10-01T19:40:41.643+0000",
            "Runtime": "python3.11",
            "Description": ""
        }
    ]
}
```

Pour plus d'informations, consultez Configurer la mémoire de fonction Lambda dans le Guide du développeur AWS Lambda.

- Pour plus de détails sur l'API, voir ListFunctions dans AWS CLI Référence de commande.

Go

Kit SDK pour Go V2

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import (
 "bytes"
 "context"
 "encoding/json"
 "errors"
 "log"
 "time"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/service/lambda"
 "github.com/aws/aws-sdk-go-v2/service/lambda/types"
)
```

```
// FunctionWrapper encapsulates function actions used in the examples.
// It contains an AWS Lambda service client that is used to perform user actions.
type FunctionWrapper struct {
 LambdaClient *lambda.Client
}



// ListFunctions lists up to maxItems functions for the account. This function
 uses a
// lambda.ListFunctionsPaginator to paginate the results.
func (wrapper FunctionWrapper) ListFunctions(ctx context.Context, maxItems int)
 []types.FunctionConfiguration {
 var functions []types.FunctionConfiguration
 paginator := lambda.NewListFunctionsPaginator(wrapper.LambdaClient,
 &lambda.ListFunctionsInput{
  MaxItems: aws.Int32(int32(maxItems)),
 })
 for paginator.HasMorePages() && len(functions) < maxItems {
  pageOutput, err := paginator.NextPage(ctx)
  if err != nil {
   log.Panicf("Couldn't list functions for your account. Here's why: %v\n", err)
  }
  functions = append(functions, pageOutput.Functions...)
 }
 return functions
}
```

- Pour plus de détails sur l'API, voir ListFunctions dans AWS SDK pour Go Référence d'API.

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
const listFunctions = () => {
  const client = new LambdaClient({});
  const command = new ListFunctionsCommand({});

  return client.send(command);
};
```

- Pour plus de détails sur l'API, voir ListFunctions dans AWS SDK pour JavaScript Référence d'API.

PHP

Kit SDK pour PHP

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    public function listFunctions($maxItems = 50, $marker = null)
    {
        if (is_null($marker)) {
            return $this->lambdaClient->listFunctions([
                'MaxItems' => $maxItems,
            ]);
        }

        return $this->lambdaClient->listFunctions([
            'Marker' => $marker,
            'MaxItems' => $maxItems,
        ]);
    }
```

- Pour plus de détails sur l'API, voir ListFunctions dans AWS SDK pour PHP Référence d'API.

PowerShell

Outils pour PowerShell V4

Exemple 1 : cet exemple affiche toutes les fonctions Lambda avec une taille de code triée

```
Get-LMFunctionList | Sort-Object -Property CodeSize | Select-Object FunctionName,
 RunTime, Timeout, CodeSize
```

Sortie :

```
FunctionName                                                    Runtime   Timeout
 CodeSize
------------                                                    -------   -------
 --------
test                                                            python2.7       3
   243
MylambdaFunction123                                             python3.8     600
   659
myfuncpython1                                                   python3.8     303
   675
```

- Pour plus de détails sur l'API, voir ListFunctions dans Outils AWS pour PowerShell Référence de l'applet de commande (V4).

Outils pour PowerShell V5

Exemple 1 : cet exemple affiche toutes les fonctions Lambda avec une taille de code triée

```
Get-LMFunctionList | Sort-Object -Property CodeSize | Select-Object FunctionName,
 RunTime, Timeout, CodeSize
```

Sortie :

```
FunctionName                                                    Runtime   Timeout
 CodeSize
------------                                                    -------   -------
 --------
test                                                            python2.7       3
   243
MylambdaFunction123                                             python3.8     600
   659
```

```
myfuncpython1                                                    python3.8     303
   675
```

- Pour plus de détails sur l'API, voir ListFunctions dans Outils AWS pour PowerShell Référence de l'applet de commande (V5).

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class LambdaWrapper:
    def __init__(self, lambda_client, iam_resource):
        self.lambda_client = lambda_client
        self.iam_resource = iam_resource


    def list_functions(self):
        """
        Lists the Lambda functions for the current account.
        """
        try:
            func_paginator = self.lambda_client.get_paginator("list_functions")
            for func_page in func_paginator.paginate():
                for func in func_page["Functions"]:
                    print(func["FunctionName"])
                    desc = func.get("Description")
                    if desc:
                        print(f"\t{desc}")
                    print(f"\t{func['Runtime']}: {func['Handler']}")
        except ClientError as err:
            logger.error(
                "Couldn't list functions. Here's why: %s: %s",
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
```

```
            raise
```

- Pour plus de détails sur l'API, voir ListFunctions dans AWS Référence de l'API du SDK pour Python (Boto3).

Ruby

Kit SDK pour Ruby

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class LambdaWrapper
  attr_accessor :lambda_client, :cloudwatch_client, :iam_client

  def initialize
    @lambda_client = Aws::Lambda::Client.new
    @cloudwatch_client = Aws::CloudWatchLogs::Client.new(region: 'us-east-1')
    @iam_client = Aws::IAM::Client.new(region: 'us-east-1')
    @logger = Logger.new($stdout)
    @logger.level = Logger::WARN
  end

  # Lists the Lambda functions for the current account.
  def list_functions
    functions = []
    @lambda_client.list_functions.each do |response|
      response['functions'].each do |function|
        functions.append(function['function_name'])
      end
    end
    functions
  rescue Aws::Lambda::Errors::ServiceException => e
    @logger.error("There was an error listing functions:\n #{e.message}")
  end
```

- Pour plus de détails sur l'API, voir ListFunctions dans AWS SDK pour Ruby Référence d'API.

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    /** List all Lambda functions in the current Region. */
    pub async fn list_functions(&self) -> Result<ListFunctionsOutput,
anyhow::Error> {
        info!("Listing lambda functions");
        self.lambda_client
            .list_functions()
            .send()
            .await
            .map_err(anyhow::Error::from)
    }
```

- Pour plus de détails sur l'API, voir ListFunctions dans AWS Référence de l'API SDK pour Rust.

SAP ABAP

Kit SDK pour SAP ABAP

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    TRY.
```

```
        oo_result = lo_lmd->listfunctions( ).       " oo_result is returned for
testing purposes. "
        DATA(lt_functions) = oo_result->get_functions( ).
        MESSAGE 'Retrieved list of Lambda functions.' TYPE 'I'.
      CATCH /aws1/cx_lmdinvparamvalueex.
        MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
      CATCH /aws1/cx_lmdserviceexception.
        MESSAGE 'An internal problem was encountered by the AWS Lambda service.'
TYPE 'E'.
      CATCH /aws1/cx_lmdtoomanyrequestsex.
        MESSAGE 'The maximum request throughput was reached.' TYPE 'E'.
    ENDTRY.
```

- Pour plus de détails sur l'API, voir ListFunctions dans AWS Référence du SDK pour l'API SAP ABAP.

Swift

Kit SDK pour Swift

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import AWSClientRuntime
import AWSLambda
import Foundation

    /// Returns an array containing the names of all AWS Lambda functions
    /// available to the user.
    ///
    /// - Parameter lambdaClient: The `IAMClient` to use.
    ///
    /// - Throws: `ExampleError.listFunctionsError`
    ///
    /// - Returns: An array of lambda function name strings.
    func getFunctionNames(lambdaClient: LambdaClient) async throws -> [String] {
        let pages = lambdaClient.listFunctionsPaginated(
```

```
            input: ListFunctionsInput()
        )

        var functionNames: [String] = []

        for try await page in pages {
            guard let functions = page.functions else {
                throw ExampleError.listFunctionsError
            }

            for function in functions {
                functionNames.append(function.functionName ?? "<unknown>")
            }
        }

        return functionNames
    }
```

- Pour plus de détails sur l'API, voir ListFunctions dans AWS Référence du SDK pour l'API Swift.

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Utilisation de **`ListProvisionedConcurrencyConfigs`** avec une CLI

Les exemples de code suivants illustrent comment utiliser `ListProvisionedConcurrencyConfigs`.

CLI

AWS CLI

Pour obtenir une liste des configurations de simultanéité allouée

L'exemple `list-provisioned-concurrency-configs` suivant répertorie les configurations de simultanéité allouée pour la fonction spécifiée.

```
aws lambda list-provisioned-concurrency-configs \
    --function-name my-function
```

Sortie :

```
{
    "ProvisionedConcurrencyConfigs": [
        {
            "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-
function:GREEN",
            "RequestedProvisionedConcurrentExecutions": 100,
            "AvailableProvisionedConcurrentExecutions": 100,
            "AllocatedProvisionedConcurrentExecutions": 100,
            "Status": "READY",
            "LastModified": "2019-12-31T20:29:00+0000"
        },
        {
            "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-
function:BLUE",
            "RequestedProvisionedConcurrentExecutions": 100,
            "AvailableProvisionedConcurrentExecutions": 100,
            "AllocatedProvisionedConcurrentExecutions": 100,
            "Status": "READY",
            "LastModified": "2019-12-31T20:28:49+0000"
        }
    ]
}
```

Pour plus d'informations, voir Configuration de la simultanéité provisionnée pour une fonction événementielle dans le AWS Guide du développeur Lambda.

- Pour plus de détails sur l'API, voir ListProvisionedConcurrencyConfigs dans AWS CLI Référence de commande.

PowerShell

Outils pour PowerShell V4

Exemple 1 : cet exemple récupère la liste des configurations de la simultanéité allouée pour une fonction Lambda.

```
Get-LMProvisionedConcurrencyConfigList -FunctionName "MylambdaFunction123"
```

- Pour plus de détails sur l'API, voir ListProvisionedConcurrencyConfigs dans Outils AWS pour PowerShell Référence de l'applet de commande (V4).

Outils pour PowerShell V5

Exemple 1 : cet exemple récupère la liste des configurations de la simultanéité allouée pour une fonction Lambda.

```
Get-LMProvisionedConcurrencyConfigList -FunctionName "MylambdaFunction123"
```

- Pour plus de détails sur l'API, voir ListProvisionedConcurrencyConfigs dans Outils AWS pour PowerShell Référence de l'applet de commande (V5).

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Utilisation de **`ListTags`** avec une CLI

Les exemples de code suivants illustrent comment utiliser `ListTags`.

CLI

AWS CLI

Pour récupérer la liste des balises d'une fonction Lambda

L'exemple `list-tags` suivant affiche les balises associées à la fonction Lambda `my-function`.

```
aws lambda list-tags \
    --resource arn:aws:lambda:us-west-2:123456789012:function:my-function
```

Sortie :

```
{
    "Tags": {
        "Category": "Web Tools",
        "Department": "Sales"
    }
}
```

Pour plus d'informations, consultez Étiquetage des fonctions Lambda dans le Guide du développeur AWS .

- Pour plus de détails sur l'API, voir ListTags dans AWS CLI Référence de commande.

PowerShell

Outils pour PowerShell V4

Exemple 1 : récupère les balises et leurs valeurs actuellement définies sur la fonction spécifiée.

```
Get-LMResourceTag -Resource "arn:aws:lambda:us-
west-2:123456789012:function:MyFunction"
```

Sortie :

```
Key        Value
---        -----
California Sacramento
Oregon     Salem
Washington Olympia
```

- Pour plus de détails sur l'API, voir ListTags dans Outils AWS pour PowerShell Référence de l'applet de commande (V4).

Outils pour PowerShell V5

Exemple 1 : récupère les balises et leurs valeurs actuellement définies sur la fonction spécifiée.

```
Get-LMResourceTag -Resource "arn:aws:lambda:us-
west-2:123456789012:function:MyFunction"
```

Sortie :

```
Key        Value
---        -----
California Sacramento
Oregon     Salem
Washington Olympia
```

- Pour plus de détails sur l'API, voir ListTags dans Outils AWS pour PowerShell Référence de l'applet de commande (V5).

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Utilisation de **`ListVersionsByFunction`** avec une CLI

Les exemples de code suivants illustrent comment utiliser `ListVersionsByFunction`.

CLI

AWS CLI

Pour récupérer la liste des versions d'une fonction

L'exemple `list-versions-by-function` suivant affiche la liste des versions de la fonction Lambda `my-function`.

```
aws lambda list-versions-by-function \
    --function-name my-function
```

Sortie :

```
{
    "Versions": [
        {
            "TracingConfig": {
                "Mode": "PassThrough"
            },
            "Version": "$LATEST",
            "CodeSha256": "sU0cJ2/hOZevwV/lTxCuQqK3gDZP3i8gUoqUUVRmY6E=",
            "FunctionName": "my-function",
            "VpcConfig": {
                "SubnetIds": [],
                "VpcId": "",
                "SecurityGroupIds": []
            },
            "MemorySize": 256,
            "RevisionId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "CodeSize": 266,
            "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-
function:$LATEST",
            "Handler": "index.handler",
```

```
            "Role": "arn:aws:iam::123456789012:role/service-role/
helloWorldPython-role-uy3l9qyq",
            "Timeout": 3,
            "LastModified": "2019-10-01T16:47:28.490+0000",
            "Runtime": "nodejs10.x",
            "Description": ""
        },
        {
            "TracingConfig": {
                "Mode": "PassThrough"
            },
            "Version": "1",
            "CodeSha256": "5tT2qgzYUHoqwR616pZ2dpkn/0J1FrzJmlKidWaaCgk=",
            "FunctionName": "my-function",
            "VpcConfig": {
                "SubnetIds": [],
                "VpcId": "",
                "SecurityGroupIds": []
            },
            "MemorySize": 256,
            "RevisionId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
            "CodeSize": 304,
            "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-
function:1",
            "Handler": "index.handler",
            "Role": "arn:aws:iam::123456789012:role/service-role/
helloWorldPython-role-uy3l9qyq",
            "Timeout": 3,
            "LastModified": "2019-09-26T20:28:40.438+0000",
            "Runtime": "nodejs10.x",
            "Description": "new version"
        },
        {
            "TracingConfig": {
                "Mode": "PassThrough"
            },
            "Version": "2",
            "CodeSha256": "sU0cJ2/hOZevwV/lTxCuQqK3gDZP3i8gUoqUUVRmY6E=",
            "FunctionName": "my-function",
            "VpcConfig": {
                "SubnetIds": [],
                "VpcId": "",
                "SecurityGroupIds": []
            },
```

```
            "MemorySize": 256,
            "RevisionId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
            "CodeSize": 266,
            "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-
function:2",
            "Handler": "index.handler",
            "Role": "arn:aws:iam::123456789012:role/service-role/
helloWorldPython-role-uy3l9qyq",
            "Timeout": 3,
            "LastModified": "2019-10-01T16:47:28.490+0000",
            "Runtime": "nodejs10.x",
            "Description": "newer version"
        }
    ]
}
```

Pour plus d'informations, voir Configuration AWS Alias de fonctions Lambda dans le AWS Guide du développeur Lambda.

- Pour plus de détails sur l'API, voir ListVersionsByFunction dans AWS CLI Référence de commande.

PowerShell

Outils pour PowerShell V4

Exemple 1 : cet exemple renvoie la liste des configurations spécifiques à chaque version de la fonction Lambda.

```
Get-LMVersionsByFunction -FunctionName "MylambdaFunction123"
```

Sortie :

```
FunctionName        Runtime   MemorySize Timeout CodeSize LastModified
      RoleName
------------        -------   ---------- ------- -------- ------------
      --------
MylambdaFunction123 python3.8        128     600      659
 2020-01-10T03:20:56.390+0000 lambda
MylambdaFunction123 python3.8        128       5     1426
 2019-12-25T09:19:02.238+0000 lambda
```

```
MylambdaFunction123 python3.8        128       5     1426
 2019-12-25T09:39:36.779+0000 lambda
MylambdaFunction123 python3.8        128     600     1426
 2019-12-25T09:52:59.872+0000 lambda
```

- Pour plus de détails sur l'API, voir ListVersionsByFunction dans Outils AWS pour PowerShell Référence de l'applet de commande (V4).

Outils pour PowerShell V5

Exemple 1 : cet exemple renvoie la liste des configurations spécifiques à chaque version de la fonction Lambda.

```
Get-LMVersionsByFunction -FunctionName "MylambdaFunction123"
```

Sortie :

```
FunctionName        Runtime   MemorySize Timeout CodeSize LastModified
      RoleName
------------        -------   ---------- ------- -------- ------------
      --------
MylambdaFunction123 python3.8        128     600      659
 2020-01-10T03:20:56.390+0000 lambda
MylambdaFunction123 python3.8        128       5     1426
 2019-12-25T09:19:02.238+0000 lambda
MylambdaFunction123 python3.8        128       5     1426
 2019-12-25T09:39:36.779+0000 lambda
MylambdaFunction123 python3.8        128     600     1426
 2019-12-25T09:52:59.872+0000 lambda
```

- Pour plus de détails sur l'API, voir ListVersionsByFunction dans Outils AWS pour PowerShell Référence de l'applet de commande (V5).

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Utilisation de **`PublishVersion`** avec une CLI

Les exemples de code suivants illustrent comment utiliser `PublishVersion`.

CLI

AWS CLI

Pour publier une nouvelle version d'une fonction

L'exemple `publish-version` suivant publie une nouvelle version de la fonction Lambda `my-function`.

```
aws lambda publish-version \
    --function-name my-function
```

Sortie :

```
{
    "TracingConfig": {
        "Mode": "PassThrough"
    },
    "CodeSha256": "dBG9m8SGdmlEjw/JYXlhhvCrAv5TxvXsbL/RMr0fT/I=",
    "FunctionName": "my-function",
    "CodeSize": 294,
    "RevisionId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "MemorySize": 128,
    "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-
function:3",
    "Version": "2",
    "Role": "arn:aws:iam::123456789012:role/service-role/MyTestFunction-role-
zgur6bf4",
    "Timeout": 3,
    "LastModified": "2019-09-23T18:32:33.857+0000",
    "Handler": "my-function.handler",
    "Runtime": "nodejs10.x",
    "Description": ""
}
```

Pour plus d'informations, voir Configuration AWS Alias de fonctions Lambda dans le AWS Guide du développeur Lambda.

- Pour plus de détails sur l'API, voir PublishVersion dans AWS CLI Référence de commande.

PowerShell

Outils pour PowerShell V4

Exemple 1 : cet exemple crée une version pour l'instantané existant du code de fonction Lambda

```
Publish-LMVersion -FunctionName "MylambdaFunction123" -Description "Publishing
 Existing Snapshot of function code as a  new version through Powershell"
```

- Pour plus de détails sur l'API, voir PublishVersion dans Outils AWS pour PowerShell Référence de l'applet de commande (V4).

Outils pour PowerShell V5

Exemple 1 : cet exemple crée une version pour l'instantané existant du code de fonction Lambda

```
Publish-LMVersion -FunctionName "MylambdaFunction123" -Description "Publishing
 Existing Snapshot of function code as a  new version through Powershell"
```

- Pour plus de détails sur l'API, voir PublishVersion dans Outils AWS pour PowerShell Référence de l'applet de commande (V5).

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Utilisation de **`PutFunctionConcurrency`** avec une CLI

Les exemples de code suivants illustrent comment utiliser `PutFunctionConcurrency`.

CLI

AWS CLI

Pour configurer une limite de simultanéité réservée pour une fonction

L'exemple `put-function-concurrency` suivant configure 100 exécutions simultanées réservées pour la fonction `my-function`.

```
aws lambda put-function-concurrency \
    --function-name  my-function  \
    --reserved-concurrent-executions 100
```

Sortie :

```
{
    "ReservedConcurrentExecutions": 100
}
```

Pour plus d'informations, consultez Réservation de simultanéité pour une fonction Lambda dans le Guide du développeur AWS Lambda.

- Pour plus de détails sur l'API, voir PutFunctionConcurrency dans AWS CLI Référence de commande.

PowerShell

Outils pour PowerShell V4

Exemple 1 : cet exemple applique les paramètres de simultanéité pour la fonction dans son ensemble.

```
Write-LMFunctionConcurrency -FunctionName "MylambdaFunction123" -
ReservedConcurrentExecution 100
```

- Pour plus de détails sur l'API, voir PutFunctionConcurrency dans Outils AWS pour PowerShell Référence de l'applet de commande (V4).

Outils pour PowerShell V5

Exemple 1 : cet exemple applique les paramètres de simultanéité pour la fonction dans son ensemble.

```
Write-LMFunctionConcurrency -FunctionName "MylambdaFunction123" -
ReservedConcurrentExecution 100
```

- Pour plus de détails sur l'API, voir PutFunctionConcurrency dans Outils AWS pour PowerShell Référence de l'applet de commande (V5).

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Utilisation de **`PutProvisionedConcurrencyConfig`** avec une CLI

Les exemples de code suivants illustrent comment utiliser `PutProvisionedConcurrencyConfig`.

CLI

AWS CLI

Pour allouer une simultanéité allouée

L'exemple `put-provisioned-concurrency-config` suivant alloue 100 simultanéités allouées à l'alias `BLUE` de la fonction spécifiée.

```
aws lambda put-provisioned-concurrency-config \
    --function-name my-function \
    --qualifier BLUE \
    --provisioned-concurrent-executions 100
```

Sortie :

```
{
    "RequestedProvisionedConcurrentExecutions": 100,
    "AllocatedProvisionedConcurrentExecutions": 0,
    "Status": "IN_PROGRESS",
    "LastModified": "2019-11-21T19:32:12+0000"
}
```

Pour plus d'informations, voir Configuration de la simultanéité provisionnée pour une fonction événementielle dans le AWS Guide du développeur Lambda.

- Pour plus de détails sur l'API, voir PutProvisionedConcurrencyConfig dans AWS CLI Référence de commande.

PowerShell

Outils pour PowerShell V4

Exemple 1 : cet exemple ajoute une configuration de simultanéité allouée à l'alias d'une fonction

```
Write-LMProvisionedConcurrencyConfig -FunctionName "MylambdaFunction123" -
ProvisionedConcurrentExecution 20 -Qualifier "NewAlias1"
```

- Pour plus de détails sur l'API, voir PutProvisionedConcurrencyConfig dans Outils AWS pour PowerShell Référence de l'applet de commande (V4).

Outils pour PowerShell V5

Exemple 1 : cet exemple ajoute une configuration de simultanéité allouée à l'alias d'une fonction

```
Write-LMProvisionedConcurrencyConfig -FunctionName "MylambdaFunction123" -
ProvisionedConcurrentExecution 20 -Qualifier "NewAlias1"
```

- Pour plus de détails sur l'API, voir PutProvisionedConcurrencyConfig dans Outils AWS pour PowerShell Référence de l'applet de commande (V5).

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Utilisation de **`RemovePermission`** avec une CLI

Les exemples de code suivants illustrent comment utiliser `RemovePermission`.

CLI

AWS CLI

Pour supprimer les autorisations d'une fonction Lambda existante

L'exemple `remove-permission` retire l'autorisation d'invoquer une fonction nommée `my-function`.

```
aws lambda remove-permission \
    --function-name my-function \
    --statement-id sns
```

Cette commande ne produit aucune sortie.

Pour plus d'informations, voir En utilisant Resource-based Politiques pour AWS Lambda dans le AWS Guide du développeur Lambda.

- Pour plus de détails sur l'API, voir RemovePermission dans AWS CLI Référence de commande.

PowerShell

Outils pour PowerShell V4

Exemple 1 : Cet exemple supprime la politique de fonction pour le paramètre spécifié StatementId d'une fonction Lambda.

```
$policy =  Get-LMPolicy -FunctionName "MylambdaFunction123" -Select Policy |
 ConvertFrom-Json| Select-Object -ExpandProperty Statement
Remove-LMPermission -FunctionName "MylambdaFunction123" -StatementId
 $policy[0].Sid
```

- Pour plus de détails sur l'API, voir RemovePermission dans Outils AWS pour PowerShell Référence de l'applet de commande (V4).

Outils pour PowerShell V5

Exemple 1 : Cet exemple supprime la politique de fonction pour le paramètre spécifié StatementId d'une fonction Lambda.

```
$policy =  Get-LMPolicy -FunctionName "MylambdaFunction123" -Select Policy |
 ConvertFrom-Json| Select-Object -ExpandProperty Statement
Remove-LMPermission -FunctionName "MylambdaFunction123" -StatementId
 $policy[0].Sid
```

- Pour plus de détails sur l'API, voir RemovePermission dans Outils AWS pour PowerShell Référence de l'applet de commande (V5).

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Utilisation de **`TagResource`** avec une CLI

Les exemples de code suivants illustrent comment utiliser `TagResource`.

CLI

AWS CLI

Pour ajouter des balises à une fonction Lambda existante

L'exemple `tag-resource` suivant ajoute une balise avec le nom de clé `DEPARTMENT` et la valeur `Department A` à la fonction Lambda spécifiée.

```
aws lambda tag-resource \
    --resource arn:aws:lambda:us-west-2:123456789012:function:my-function \
    --tags "DEPARTMENT=Department A"
```

Cette commande ne produit aucune sortie.

Pour plus d'informations, consultez Étiquetage des fonctions Lambda dans le Guide du développeur AWS .

- Pour plus de détails sur l'API, voir TagResource dans AWS CLI Référence de commande.

PowerShell

Outils pour PowerShell V4

Exemple 1 : ajoute les trois balises (Washington, Oregon et Californie) et leurs valeurs associées à la fonction spécifiée identifiée par son ARN.

```
Add-LMResourceTag -Resource "arn:aws:lambda:us-
west-2:123456789012:function:MyFunction" -Tag @{ "Washington" = "Olympia";
 "Oregon" = "Salem"; "California" = "Sacramento" }
```

- Pour plus de détails sur l'API, voir TagResource dans Outils AWS pour PowerShell Référence de l'applet de commande (V4).

Outils pour PowerShell V5

Exemple 1 : ajoute les trois balises (Washington, Oregon et Californie) et leurs valeurs associées à la fonction spécifiée identifiée par son ARN.

```
Add-LMResourceTag -Resource "arn:aws:lambda:us-
west-2:123456789012:function:MyFunction" -Tag @{ "Washington" = "Olympia";
 "Oregon" = "Salem"; "California" = "Sacramento" }
```

- Pour plus de détails sur l'API, voir TagResource dans Outils AWS pour PowerShell Référence de l'applet de commande (V5).

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Utilisation de **`UntagResource`** avec une CLI

Les exemples de code suivants illustrent comment utiliser `UntagResource`.

CLI

AWS CLI

Pour supprimer les balises d'une fonction Lambda existante

L'exemple `untag-resource` suivant supprime la balise dont la clé est `DEPARTMENT` de la fonction Lambda `my-function`.

```
aws lambda untag-resource \
    --resource arn:aws:lambda:us-west-2:123456789012:function:my-function \
    --tag-keys DEPARTMENT
```

Cette commande ne produit aucune sortie.

Pour plus d'informations, consultez Étiquetage des fonctions Lambda dans le Guide du développeur AWS .

- Pour plus de détails sur l'API, voir UntagResource dans AWS CLI Référence de commande.

PowerShell

Outils pour PowerShell V4

Exemple 1 : supprime les balises fournies d'une fonction. L'applet de commande vous invitera à confirmer avant de poursuivre, à moins que l'option -Force ne soit spécifiée. Un seul appel est envoyé au service pour supprimer les tags.

```
Remove-LMResourceTag -Resource "arn:aws:lambda:us-
west-2:123456789012:function:MyFunction" -TagKey
 "Washington","Oregon","California"
```

Exemple 2 : supprime les balises fournies d'une fonction. L'applet de commande vous invitera à confirmer avant de poursuivre, à moins que l'option -Force ne soit spécifiée. Un seul appel au service est effectué par tag fourni.

```
"Washington","Oregon","California" | Remove-LMResourceTag -Resource
 "arn:aws:lambda:us-west-2:123456789012:function:MyFunction"
```

- Pour plus de détails sur l'API, voir UntagResource dans Outils AWS pour PowerShell Référence de l'applet de commande (V4).

Outils pour PowerShell V5

Exemple 1 : supprime les balises fournies d'une fonction. L'applet de commande vous invitera à confirmer avant de poursuivre, à moins que l'option -Force ne soit spécifiée. Un seul appel est envoyé au service pour supprimer les tags.

```
Remove-LMResourceTag -Resource "arn:aws:lambda:us-
west-2:123456789012:function:MyFunction" -TagKey
 "Washington","Oregon","California"
```

Exemple 2 : supprime les balises fournies d'une fonction. L'applet de commande vous invitera à confirmer avant de poursuivre, à moins que l'option -Force ne soit spécifiée. Un seul appel au service est effectué par tag fourni.

```
"Washington","Oregon","California" | Remove-LMResourceTag -Resource
 "arn:aws:lambda:us-west-2:123456789012:function:MyFunction"
```

- Pour plus de détails sur l'API, voir UntagResource dans Outils AWS pour PowerShell Référence de l'applet de commande (V5).

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Utilisation de **`UpdateAlias`** avec une CLI

Les exemples de code suivants illustrent comment utiliser `UpdateAlias`.

CLI

AWS CLI

Pour mettre à jour un alias de fonction

L'exemple `update-alias` suivant met à jour l'alias de fonction Lambda nommé `LIVE` pour qu'il pointe vers la version 3 de la fonction Lambda `my-function`.

```
aws lambda update-alias \
    --function-name my-function \
    --function-version 3 \
    --name LIVE
```

Sortie :

```
{
    "FunctionVersion": "3",
    "Name": "LIVE",
    "AliasArn": "arn:aws:lambda:us-west-2:123456789012:function:my-
function:LIVE",
    "RevisionId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Description": "alias for live version of function"
}
```

Pour plus d'informations, voir Configuration AWS Alias de fonctions Lambda dans le AWS Guide du développeur Lambda.

- Pour plus de détails sur l'API, voir UpdateAlias dans AWS CLI Référence de commande.

PowerShell

Outils pour PowerShell V4

Exemple 1 : cet exemple met à jour la configuration d'un alias de fonction Lambda existant. Il met à jour le RoutingConfiguration valeur permettant de transférer 60 % (0,6) du trafic vers la version 1

```
Update-LMAlias -FunctionName "MylambdaFunction123" -Description
 " Alias for version 2" -FunctionVersion 2 -Name "newlabel1" -
RoutingConfig_AdditionalVersionWeight @{Name="1";Value="0.6}
```

- Pour plus de détails sur l'API, voir UpdateAlias dans Outils AWS pour PowerShell Référence de l'applet de commande (V4).

Outils pour PowerShell V5

Exemple 1 : cet exemple met à jour la configuration d'un alias de fonction Lambda existant. Il met à jour le RoutingConfiguration valeur permettant de transférer 60 % (0,6) du trafic vers la version 1

```
Update-LMAlias -FunctionName "MylambdaFunction123" -Description
 " Alias for version 2" -FunctionVersion 2 -Name "newlabel1" -
RoutingConfig_AdditionalVersionWeight @{Name="1";Value="0.6}
```

- Pour plus de détails sur l'API, voir UpdateAlias dans Outils AWS pour PowerShell Référence de l'applet de commande (V5).

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Utiliser **`UpdateFunctionCode`** avec un AWS SDK ou CLI

Les exemples de code suivants illustrent comment utiliser `UpdateFunctionCode`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l'exemple de code suivant :

- Principes de base

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    /// <summary>
    /// Update an existing Lambda function.
    /// </summary>
    /// <param name="functionName">The name of the Lambda function to update.</
param>
    /// <param name="bucketName">The bucket where the zip file containing
    /// the Lambda function code is stored.</param>
    /// <param name="key">The key name of the source code file.</param>
    /// <returns>Async Task.</returns>
    public async Task UpdateFunctionCodeAsync(
        string functionName,
        string bucketName,
        string key)
    {
        var functionCodeRequest = new UpdateFunctionCodeRequest
        {
            FunctionName = functionName,
            Publish = true,
            S3Bucket = bucketName,
            S3Key = key,
        };

        var response = await
 _lambdaService.UpdateFunctionCodeAsync(functionCodeRequest);
        Console.WriteLine($"The Function was last modified at
 {response.LastModified}.");
    }
```

- Pour plus de détails sur l'API, voir UpdateFunctionCode dans AWS SDK pour .NET Référence d'API.

C++

SDK pour C++

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
        Aws::Client::ClientConfiguration clientConfig;
        // Optional: Set to the AWS Region in which the bucket was created
 (overrides config file).
        // clientConfig.region = "us-east-1";

    Aws::Lambda::LambdaClient client(clientConfig);

        Aws::Lambda::Model::UpdateFunctionCodeRequest request;
        request.SetFunctionName(LAMBDA_NAME);
        std::ifstream ifstream(CALCULATOR_LAMBDA_CODE.c_str(),
                               std::ios_base::in | std::ios_base::binary);
        if (!ifstream.is_open()) {
            std::cerr << "Error opening file " << INCREMENT_LAMBDA_CODE << "." <<
 std::endl;

#if USE_CPP_LAMBDA_FUNCTION
            std::cerr
                    << "The cpp Lambda function must be built following the
 instructions in the cpp_lambda/README.md file. "
                    << std::endl;
#endif
            deleteLambdaFunction(client);
            deleteIamRole(clientConfig);
            return false;
        }

        Aws::StringStream buffer;
        buffer << ifstream.rdbuf();
        request.SetZipFile(
                Aws::Utils::ByteBuffer((unsigned char *) buffer.str().c_str(),
                                       buffer.str().length()));
        request.SetPublish(true);
```

```
        Aws::Lambda::Model::UpdateFunctionCodeOutcome outcome =
 client.UpdateFunctionCode(
                request);

        if (outcome.IsSuccess()) {
            std::cout << "The lambda code was successfully updated." <<
 std::endl;
        }
        else {
            std::cerr << "Error with Lambda::UpdateFunctionCode. "
                      << outcome.GetError().GetMessage()
                      << std::endl;
        }
```

- Pour plus de détails sur l'API, voir UpdateFunctionCode dans AWS SDK pour C++ Référence d'API.

CLI

AWS CLI

Pour mettre à jour le code d'une fonction Lambda

L'exemple `update-function-code` suivant remplace le code de la version non publiée ($LATEST) de la fonction `my-function` par le contenu du fichier zip spécifié.

```
aws lambda update-function-code \
    --function-name  my-function \
    --zip-file fileb://my-function.zip
```

Sortie :

```
{
    "FunctionName": "my-function",
    "LastModified": "2019-09-26T20:28:40.438+0000",
    "RevisionId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "MemorySize": 256,
    "Version": "$LATEST",
    "Role": "arn:aws:iam::123456789012:role/service-role/my-function-role-
uy3l9qyq",
```

```
    "Timeout": 3,
    "Runtime": "nodejs10.x",
    "TracingConfig": {
        "Mode": "PassThrough"
    },
    "CodeSha256": "5tT2qgzYUHaqwR716pZ2dpkn/0J1FrzJmlKidWoaCgk=",
    "Description": "",
    "VpcConfig": {
        "SubnetIds": [],
        "VpcId": "",
        "SecurityGroupIds": []
    },
    "CodeSize": 304,
    "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-function",
    "Handler": "index.handler"
}
```

Pour plus d'informations, consultez Configuration des options de fonction Lambda AWS dans le Guide du développeur AWS .

- Pour plus de détails sur l'API, voir UpdateFunctionCode dans AWS CLI Référence de commande.

Go

Kit SDK pour Go V2

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import (
 "bytes"
 "context"
 "encoding/json"
 "errors"
 "log"
 "time"
```

```
 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/service/lambda"
 "github.com/aws/aws-sdk-go-v2/service/lambda/types"
)

// FunctionWrapper encapsulates function actions used in the examples.
// It contains an AWS Lambda service client that is used to perform user actions.
type FunctionWrapper struct {
 LambdaClient *lambda.Client
}



// UpdateFunctionCode updates the code for the Lambda function specified by
 functionName.
// The existing code for the Lambda function is entirely replaced by the code in
 the
// zipPackage buffer. After the update action is called, a
 lambda.FunctionUpdatedV2Waiter
// is used to wait until the update is successful.
func (wrapper FunctionWrapper) UpdateFunctionCode(ctx context.Context,
 functionName string, zipPackage *bytes.Buffer) types.State {
 var state types.State
 _, err := wrapper.LambdaClient.UpdateFunctionCode(ctx,
 &lambda.UpdateFunctionCodeInput{
  FunctionName: aws.String(functionName), ZipFile: zipPackage.Bytes(),
 })
 if err != nil {
  log.Panicf("Couldn't update code for function %v. Here's why: %v\n",
 functionName, err)
 } else {
  waiter := lambda.NewFunctionUpdatedV2Waiter(wrapper.LambdaClient)
  funcOutput, err := waiter.WaitForOutput(ctx, &lambda.GetFunctionInput{
   FunctionName: aws.String(functionName)}, 1*time.Minute)
  if err != nil {
   log.Panicf("Couldn't wait for function %v to be active. Here's why: %v\n",
 functionName, err)
  } else {
   state = funcOutput.Configuration.State
  }
 }
 return state
}
```

- Pour plus de détails sur l'API, voir UpdateFunctionCode dans AWS SDK pour Go Référence d'API.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
   /**
    * Updates the code for an AWS Lambda function.
    *
    * @param awsLambda  the AWS Lambda client
    * @param functionName the name of the Lambda function to update
    * @param bucketName the name of the S3 bucket where the function code is
located
    * @param key the key (file name) of the function code in the S3 bucket
    * @throws LambdaException if there is an error updating the function code
    */
   public static void updateFunctionCode(LambdaClient awsLambda, String
functionName, String bucketName, String key) {
       try {
           LambdaWaiter waiter = awsLambda.waiter();
           UpdateFunctionCodeRequest functionCodeRequest =
UpdateFunctionCodeRequest.builder()
                .functionName(functionName)
                .publish(true)
                .s3Bucket(bucketName)
                .s3Key(key)
                .build();

           UpdateFunctionCodeResponse response =
awsLambda.updateFunctionCode(functionCodeRequest);
           GetFunctionConfigurationRequest getFunctionConfigRequest =
GetFunctionConfigurationRequest.builder()
```

```
                .functionName(functionName)
                .build();

            WaiterResponse<GetFunctionConfigurationResponse> waiterResponse =
 waiter
                .waitUntilFunctionUpdated(getFunctionConfigRequest);
            waiterResponse.matched().response().ifPresent(System.out::println);
            System.out.println("The last modified value is " +
 response.lastModified());

        } catch (LambdaException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
```

- Pour plus de détails sur l'API, voir UpdateFunctionCode dans AWS SDK for Java 2.x Référence d'API.

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
const updateFunctionCode = async (funcName, newFunc) => {
  const client = new LambdaClient({});
  const code = await readFile(`${dirname}../functions/${newFunc}.zip`);
  const command = new UpdateFunctionCodeCommand({
    ZipFile: code,
    FunctionName: funcName,
    Architectures: [Architecture.arm64],
    Handler: "index.handler", // Required when sending a .zip file
    PackageType: PackageType.Zip, // Required when sending a .zip file
    Runtime: Runtime.nodejs16x, // Required when sending a .zip file
  });
```

```
  return client.send(command);
};
```

- Pour plus de détails sur l'API, voir UpdateFunctionCode dans AWS SDK pour JavaScript Référence d'API.

PHP

Kit SDK pour PHP

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    public function updateFunctionCode($functionName, $s3Bucket, $s3Key)
    {
        return $this->lambdaClient->updateFunctionCode([
            'FunctionName' => $functionName,
            'S3Bucket' => $s3Bucket,
            'S3Key' => $s3Key,
        ]);
    }
```

- Pour plus de détails sur l'API, voir UpdateFunctionCode dans AWS SDK pour PHP Référence d'API.

PowerShell

Outils pour PowerShell V4

Exemple 1 : met à jour la fonction nommée "MyFunctionavec un nouveau contenu contenu dans le fichier zip spécifié. Pour une fonction Lambda C# .NET Core, le fichier zip doit contenir l'assemblage compilé.

```
Update-LMFunctionCode -FunctionName MyFunction -ZipFilename .\UpdatedCode.zip
```

Exemple 2 : cet exemple est similaire au précédent, mais utilise un objet Amazon S3 contenant le code mis à jour pour actualiser la fonction.

```
Update-LMFunctionCode -FunctionName MyFunction -BucketName amzn-s3-demo-bucket -
Key UpdatedCode.zip
```

- Pour plus de détails sur l'API, voir UpdateFunctionCode dans Outils AWS pour PowerShell Référence de l'applet de commande (V4).

Outils pour PowerShell V5

Exemple 1 : met à jour la fonction nommée "MyFunctionavec un nouveau contenu contenu dans le fichier zip spécifié. Pour une fonction Lambda C# .NET Core, le fichier zip doit contenir l'assemblage compilé.

```
Update-LMFunctionCode -FunctionName MyFunction -ZipFilename .\UpdatedCode.zip
```

Exemple 2 : cet exemple est similaire au précédent, mais utilise un objet Amazon S3 contenant le code mis à jour pour actualiser la fonction.

```
Update-LMFunctionCode -FunctionName MyFunction -BucketName amzn-s3-demo-bucket -
Key UpdatedCode.zip
```

- Pour plus de détails sur l'API, voir UpdateFunctionCode dans Outils AWS pour PowerShell Référence de l'applet de commande (V5).

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class LambdaWrapper:
```

```
    def __init__(self, lambda_client, iam_resource):
        self.lambda_client = lambda_client
        self.iam_resource = iam_resource


    def update_function_code(self, function_name, deployment_package):
        """
        Updates the code for a Lambda function by submitting a .zip archive that
contains
        the code for the function.

        :param function_name: The name of the function to update.
        :param deployment_package: The function code to update, packaged as bytes
in
                                   .zip format.
        :return: Data about the update, including the status.
        """
        try:
            response = self.lambda_client.update_function_code(
                FunctionName=function_name, ZipFile=deployment_package
            )
        except ClientError as err:
            logger.error(
                "Couldn't update function %s. Here's why: %s: %s",
                function_name,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
        else:
            return response
```

- Pour plus de détails sur l'API, voir UpdateFunctionCode dans AWS Référence de l'API du SDK pour Python (Boto3).

Ruby

Kit SDK pour Ruby

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class LambdaWrapper
  attr_accessor :lambda_client, :cloudwatch_client, :iam_client

  def initialize
    @lambda_client = Aws::Lambda::Client.new
    @cloudwatch_client = Aws::CloudWatchLogs::Client.new(region: 'us-east-1')
    @iam_client = Aws::IAM::Client.new(region: 'us-east-1')
    @logger = Logger.new($stdout)
    @logger.level = Logger::WARN
  end

  # Updates the code for a Lambda function by submitting a .zip archive that
 contains
  # the code for the function.
  #
  # @param function_name: The name of the function to update.
  # @param deployment_package: The function code to update, packaged as bytes in
  #                            .zip format.
  # @return: Data about the update, including the status.
  def update_function_code(function_name, deployment_package)
    @lambda_client.update_function_code(
      function_name: function_name,
      zip_file: deployment_package
    )
    @lambda_client.wait_until(:function_updated_v2, { function_name:
 function_name }) do |w|
      w.max_attempts = 5
      w.delay = 5
    end
  rescue Aws::Lambda::Errors::ServiceException => e
    @logger.error("There was an error updating function code for:
 #{function_name}:\n #{e.message}")
```

```
    nil
  rescue Aws::Waiters::Errors::WaiterFailed => e
    @logger.error("Failed waiting for #{function_name} to update:\n
#{e.message}")
  end
```

- Pour plus de détails sur l'API, voir UpdateFunctionCode dans AWS SDK pour Ruby Référence d'API.

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    /** Given a Path to a zip file, update the function's code and wait for the
update to finish. */
    pub async fn update_function_code(
        &self,
        zip_file: PathBuf,
        key: String,
    ) -> Result<UpdateFunctionCodeOutput, anyhow::Error> {
        let function_code = self.prepare_function(zip_file, Some(key)).await?;

        info!("Updating code for {}", self.lambda_name);
        let update = self
            .lambda_client
            .update_function_code()
            .function_name(self.lambda_name.clone())
            .s3_bucket(self.bucket.clone())
            .s3_key(function_code.s3_key().unwrap().to_string())
            .send()
            .await
            .map_err(anyhow::Error::from)?;

        self.wait_for_function_ready().await?;
```

```
        Ok(update)
    }

    /**
     * Upload function code from a path to a zip file.
     * The zip file must have an AL2 Linux-compatible binary called `bootstrap`.
     * The easiest way to create such a zip is to use `cargo lambda build --
output-format Zip`.
     */
    async fn prepare_function(
        &self,
        zip_file: PathBuf,
        key: Option<String>,
    ) -> Result<FunctionCode, anyhow::Error> {
        let body = ByteStream::from_path(zip_file).await?;

        let key = key.unwrap_or_else(|| format!("{}_code", self.lambda_name));

        info!("Uploading function code to s3://{}/{}", self.bucket, key);
        let _ = self
            .s3_client
            .put_object()
            .bucket(self.bucket.clone())
            .key(key.clone())
            .body(body)
            .send()
            .await?;

        Ok(FunctionCode::builder()
            .s3_bucket(self.bucket.clone())
            .s3_key(key)
            .build())
    }
```

- Pour plus de détails sur l'API, voir UpdateFunctionCode dans AWS Référence de l'API SDK pour Rust.

SAP ABAP

Kit SDK pour SAP ABAP

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
   TRY.
       oo_result = lo_lmd->updatefunctioncode(     " oo_result is returned for
testing purposes. "
             iv_functionname = iv_function_name
             iv_zipfile = io_zip_file ).

       MESSAGE 'Lambda function code updated.' TYPE 'I'.
     CATCH /aws1/cx_lmdcodesigningcfgno00.
       MESSAGE 'Code signing configuration does not exist.' TYPE 'E'.
     CATCH /aws1/cx_lmdcodestorageexcdex.
       MESSAGE 'Maximum total code size per account exceeded.' TYPE 'E'.
     CATCH /aws1/cx_lmdcodeverification00.
       MESSAGE 'Code signature failed one or more validation checks for
signature mismatch or expiration.' TYPE 'E'.
     CATCH /aws1/cx_lmdinvalidcodesigex.
       MESSAGE 'Code signature failed the integrity check.' TYPE 'E'.
     CATCH /aws1/cx_lmdinvparamvalueex.
       MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
     CATCH /aws1/cx_lmdresourceconflictex.
       MESSAGE 'Resource already exists or another operation is in progress.'
TYPE 'E'.
     CATCH /aws1/cx_lmdresourcenotfoundex.
       MESSAGE 'The requested resource does not exist.' TYPE 'E'.
     CATCH /aws1/cx_lmdserviceexception.
       MESSAGE 'An internal problem was encountered by the AWS Lambda service.'
TYPE 'E'.
     CATCH /aws1/cx_lmdtoomanyrequestsex.
       MESSAGE 'The maximum request throughput was reached.' TYPE 'E'.
   ENDTRY.
```

- Pour plus de détails sur l'API, voir UpdateFunctionCode dans AWS Référence du SDK pour l'API SAP ABAP.

Swift

Kit SDK pour Swift

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import AWSClientRuntime
import AWSLambda
import Foundation

        let zipUrl = URL(fileURLWithPath: path)
        let zipData: Data

        // Read the function's Zip file.

        do {
            zipData = try Data(contentsOf: zipUrl)
        } catch {
            throw ExampleError.zipFileReadError
        }

        // Update the function's code and wait for the updated version to be
        // ready for use.

        do {
            _ = try await lambdaClient.updateFunctionCode(
                input: UpdateFunctionCodeInput(
                    functionName: functionName,
                    zipFile: zipData
                )
            )
        } catch {
            return false
        }
```

- Pour plus de détails sur l'API, voir UpdateFunctionCode dans AWS Référence du SDK pour l'API Swift.

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Utiliser **`UpdateFunctionConfiguration`** avec un AWS SDK ou CLI

Les exemples de code suivants illustrent comment utiliser `UpdateFunctionConfiguration`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l'exemple de code suivant :

- Principes de base

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
   /// <summary>
   /// Update the code of a Lambda function.
   /// </summary>
   /// <param name="functionName">The name of the function to update.</param>
   /// <param name="functionHandler">The code that performs the function's
actions.</param>
   /// <param name="environmentVariables">A dictionary of environment
variables.</param>
   /// <returns>A Boolean value indicating the success of the action.</returns>
   public async Task<bool> UpdateFunctionConfigurationAsync(
       string functionName,
```

```
        string functionHandler,
        Dictionary<string, string> environmentVariables)
    {
        var request = new UpdateFunctionConfigurationRequest
        {
            Handler = functionHandler,
            FunctionName = functionName,
            Environment = new Amazon.Lambda.Model.Environment { Variables =
environmentVariables },
        };

        var response = await
_lambdaService.UpdateFunctionConfigurationAsync(request);

        Console.WriteLine(response.LastModified);

        return response.HttpStatusCode == System.Net.HttpStatusCode.OK;
    }
```

- Pour plus de détails sur l'API, voir UpdateFunctionConfiguration dans AWS SDK pour .NET Référence d'API.

C++

SDK pour C++

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
        Aws::Client::ClientConfiguration clientConfig;
        // Optional: Set to the AWS Region in which the bucket was created
(overrides config file).
        // clientConfig.region = "us-east-1";

    Aws::Lambda::LambdaClient client(clientConfig);
```

```
        Aws::Lambda::Model::UpdateFunctionConfigurationRequest request;
        request.SetFunctionName(LAMBDA_NAME);
        Aws::Lambda::Model::Environment environment;
        environment.AddVariables("LOG_LEVEL", "DEBUG");
        request.SetEnvironment(environment);

        Aws::Lambda::Model::UpdateFunctionConfigurationOutcome outcome =
 client.UpdateFunctionConfiguration(
                request);

        if (outcome.IsSuccess()) {
            std::cout << "The lambda configuration was successfully updated."
                      << std::endl;
            break;
        }

        else {
            std::cerr << "Error with Lambda::UpdateFunctionConfiguration. "
                      << outcome.GetError().GetMessage()
                      << std::endl;
        }
```

- Pour plus de détails sur l'API, voir UpdateFunctionConfiguration dans AWS SDK pour C++ Référence d'API.

CLI

AWS CLI

Pour modifier la configuration d’une fonction

L’exemple `update-function-configuration` suivant modifie la taille de la mémoire à 256 Mo pour la version non publiée ($LATEST) de la fonction `my-function`.

```
aws lambda update-function-configuration \
    --function-name  my-function \
    --memory-size 256
```

Sortie :

```
{
```

```
    "FunctionName": "my-function",
    "LastModified": "2019-09-26T20:28:40.438+0000",
    "RevisionId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "MemorySize": 256,
    "Version": "$LATEST",
    "Role": "arn:aws:iam::123456789012:role/service-role/my-function-role-
uy3l9qyq",
    "Timeout": 3,
    "Runtime": "nodejs10.x",
    "TracingConfig": {
        "Mode": "PassThrough"
    },
    "CodeSha256": "5tT2qgzYUHaqwR716pZ2dpkn/0J1FrzJmlKidWoaCgk=",
    "Description": "",
    "VpcConfig": {
        "SubnetIds": [],
        "VpcId": "",
        "SecurityGroupIds": []
    },
    "CodeSize": 304,
    "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-function",
    "Handler": "index.handler"
}
```

Pour plus d'informations, consultez Configuration des options de fonction Lambda AWS dans le Guide du développeur AWS .

- Pour plus de détails sur l'API, voir UpdateFunctionConfiguration dans AWS CLI Référence de commande.

Go

Kit SDK pour Go V2

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import (
 "bytes"
 "context"
 "encoding/json"
 "errors"
 "log"
 "time"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/service/lambda"
 "github.com/aws/aws-sdk-go-v2/service/lambda/types"
)

// FunctionWrapper encapsulates function actions used in the examples.
// It contains an AWS Lambda service client that is used to perform user actions.
type FunctionWrapper struct {
 LambdaClient *lambda.Client
}



// UpdateFunctionConfiguration updates a map of environment variables configured
 for
// the Lambda function specified by functionName.
func (wrapper FunctionWrapper) UpdateFunctionConfiguration(ctx context.Context,
 functionName string, envVars map[string]string) {
 _, err := wrapper.LambdaClient.UpdateFunctionConfiguration(ctx,
 &lambda.UpdateFunctionConfigurationInput{
  FunctionName: aws.String(functionName),
  Environment:  &types.Environment{Variables: envVars},
 })
 if err != nil {
  log.Panicf("Couldn't update configuration for %v. Here's why: %v",
 functionName, err)
 }
}
```

- Pour plus de détails sur l'API, voir UpdateFunctionConfiguration dans AWS SDK pour Go Référence d'API.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    /**
     * Updates the configuration of an AWS Lambda function.
     *
     * @param awsLambda     the {@link LambdaClient} instance to use for the AWS
Lambda operation
     * @param functionName  the name of the AWS Lambda function to update
     * @param handler       the new handler for the AWS Lambda function
     *
     * @throws LambdaException if there is an error while updating the function
configuration
     */
    public static void updateFunctionConfiguration(LambdaClient awsLambda, String
functionName, String handler) {
        try {
            UpdateFunctionConfigurationRequest configurationRequest =
UpdateFunctionConfigurationRequest.builder()
                .functionName(functionName)
                .handler(handler)
                .runtime(Runtime.JAVA17)
                .build();

            awsLambda.updateFunctionConfiguration(configurationRequest);

        } catch (LambdaException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
```

- Pour plus de détails sur l'API, voir UpdateFunctionConfiguration dans AWS SDK for Java 2.x Référence d'API.

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
const updateFunctionConfiguration = async (funcName) => {
  const client = new LambdaClient({});
  const config = readFileSync(`${dirname}../functions/config.json`).toString();
  const command = new UpdateFunctionConfigurationCommand({
    ...JSON.parse(config),
    FunctionName: funcName,
  });
  const result = await client.send(command);
  await waitForFunctionUpdated({ FunctionName: funcName });
  return result;
};
```

- Pour plus de détails sur l'API, voir UpdateFunctionConfiguration dans AWS SDK pour JavaScript Référence d'API.

PHP

Kit SDK pour PHP

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    public function updateFunctionConfiguration($functionName, $handler,
 $environment = '')
    {
```

```
        return $this->lambdaClient->updateFunctionConfiguration([
            'FunctionName' => $functionName,
            'Handler' => "$handler.lambda_handler",
            'Environment' => $environment,
        ]);
    }
```

- Pour plus de détails sur l'API, voir UpdateFunctionConfiguration dans AWS SDK pour PHP Référence d'API.

PowerShell

Outils pour PowerShell V4

Exemple 1 : cet exemple met à jour la configuration de la fonction Lambda existante

```
Update-LMFunctionConfiguration -FunctionName "MylambdaFunction123" -Handler
 "lambda_function.launch_instance" -Timeout 600 -Environment_Variable
 @{ "envvar1"="value";"envvar2"="value" } -Role arn:aws:iam::123456789101:role/
service-role/lambda -DeadLetterConfig_TargetArn arn:aws:sns:us-east-1:
 123456789101:MyfirstTopic
```

- Pour plus de détails sur l'API, voir UpdateFunctionConfiguration dans Outils AWS pour PowerShell Référence de l'applet de commande (V4).

Outils pour PowerShell V5

Exemple 1 : cet exemple met à jour la configuration de la fonction Lambda existante

```
Update-LMFunctionConfiguration -FunctionName "MylambdaFunction123" -Handler
 "lambda_function.launch_instance" -Timeout 600 -Environment_Variable
 @{ "envvar1"="value";"envvar2"="value" } -Role arn:aws:iam::123456789101:role/
service-role/lambda -DeadLetterConfig_TargetArn arn:aws:sns:us-east-1:
 123456789101:MyfirstTopic
```

- Pour plus de détails sur l'API, voir UpdateFunctionConfiguration dans Outils AWS pour PowerShell Référence de l'applet de commande (V5).

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class LambdaWrapper:
    def __init__(self, lambda_client, iam_resource):
        self.lambda_client = lambda_client
        self.iam_resource = iam_resource


    def update_function_configuration(self, function_name, env_vars):
        """
        Updates the environment variables for a Lambda function.

        :param function_name: The name of the function to update.
        :param env_vars: A dict of environment variables to update.
        :return: Data about the update, including the status.
        """
        try:
            response = self.lambda_client.update_function_configuration(
                FunctionName=function_name, Environment={"Variables": env_vars}
            )
        except ClientError as err:
            logger.error(
                "Couldn't update function configuration %s. Here's why: %s: %s",
                function_name,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
        else:
            return response
```

- Pour plus de détails sur l'API, voir UpdateFunctionConfiguration dans AWS Référence de l'API du SDK pour Python (Boto3).

Ruby

Kit SDK pour Ruby

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class LambdaWrapper
  attr_accessor :lambda_client, :cloudwatch_client, :iam_client

  def initialize
    @lambda_client = Aws::Lambda::Client.new
    @cloudwatch_client = Aws::CloudWatchLogs::Client.new(region: 'us-east-1')
    @iam_client = Aws::IAM::Client.new(region: 'us-east-1')
    @logger = Logger.new($stdout)
    @logger.level = Logger::WARN
  end

  # Updates the environment variables for a Lambda function.
  # @param function_name: The name of the function to update.
  # @param log_level: The log level of the function.
  # @return: Data about the update, including the status.
  def update_function_configuration(function_name, log_level)
    @lambda_client.update_function_configuration({
                                                   function_name: function_name,
                                                   environment: {
                                                     variables: {
                                                       'LOG_LEVEL' => log_level
                                                     }
                                                   }
                                                 })
    @lambda_client.wait_until(:function_updated_v2, { function_name:
 function_name }) do |w|
      w.max_attempts = 5
      w.delay = 5
```

```
    end
  rescue Aws::Lambda::Errors::ServiceException => e
    @logger.error("There was an error updating configurations for
#{function_name}:\n #{e.message}")
  rescue Aws::Waiters::Errors::WaiterFailed => e
    @logger.error("Failed waiting for #{function_name} to activate:\n
#{e.message}")
  end
```

- Pour plus de détails sur l'API, voir UpdateFunctionConfiguration dans AWS SDK pour Ruby Référence d'API.

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    /** Update the environment for a function. */
    pub async fn update_function_configuration(
        &self,
        environment: Environment,
    ) -> Result<UpdateFunctionConfigurationOutput, anyhow::Error> {
        info!(
            ?environment,
            "Updating environment for {}", self.lambda_name
        );
        let updated = self
            .lambda_client
            .update_function_configuration()
            .function_name(self.lambda_name.clone())
            .environment(environment)
            .send()
            .await
            .map_err(anyhow::Error::from)?;
```

```
        self.wait_for_function_ready().await?;

        Ok(updated)
    }
```

- Pour plus de détails sur l'API, voir UpdateFunctionConfiguration dans AWS Référence de l'API SDK pour Rust.

SAP ABAP

Kit SDK pour SAP ABAP

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    TRY.
        oo_result = lo_lmd->updatefunctionconfiguration(     " oo_result is
returned for testing purposes. "
              iv_functionname = iv_function_name
              iv_runtime = iv_runtime
              iv_description  = 'Updated Lambda function'
              iv_memorysize  = iv_memory_size ).

        MESSAGE 'Lambda function configuration/settings updated.' TYPE 'I'.
      CATCH /aws1/cx_lmdcodesigningcfgno00.
        MESSAGE 'Code signing configuration does not exist.' TYPE 'E'.
      CATCH /aws1/cx_lmdcodeverification00.
        MESSAGE 'Code signature failed one or more validation checks for
signature mismatch or expiration.' TYPE 'E'.
      CATCH /aws1/cx_lmdinvalidcodesigex.
        MESSAGE 'Code signature failed the integrity check.' TYPE 'E'.
      CATCH /aws1/cx_lmdinvparamvalueex.
        MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
      CATCH /aws1/cx_lmdresourceconflictex.
        MESSAGE 'Resource already exists or another operation is in progress.'
TYPE 'E'.
      CATCH /aws1/cx_lmdresourcenotfoundex.
```

```
        MESSAGE 'The requested resource does not exist.' TYPE 'E'.
      CATCH /aws1/cx_lmdserviceexception.
        MESSAGE 'An internal problem was encountered by the AWS Lambda service.'
 TYPE 'E'.
      CATCH /aws1/cx_lmdtoomanyrequestsex.
        MESSAGE 'The maximum request throughput was reached.' TYPE 'E'.
    ENDTRY.
```

- Pour plus de détails sur l'API, voir UpdateFunctionConfiguration dans AWS Référence du SDK pour l'API SAP ABAP.

Swift

Kit SDK pour Swift

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import AWSClientRuntime
import AWSLambda
import Foundation

    /// Tell the server-side component to log debug output by setting its
    /// environment's `LOG_LEVEL` to `DEBUG`.
    ///
    /// - Parameters:
    ///   - lambdaClient: The `LambdaClient` to use.
    ///   - functionName: The name of the AWS Lambda function to enable debug
    ///     logging for.
    ///
    /// - Throws: `ExampleError.environmentResponseMissingError`,
    ///   `ExampleError.updateFunctionConfigurationError`,
    ///   `ExampleError.environmentVariablesMissingError`,
    ///   `ExampleError.logLevelIncorrectError`,
    ///   `ExampleError.updateFunctionConfigurationError`
    func enableDebugLogging(lambdaClient: LambdaClient, functionName: String)
 async throws {
```

```
        let envVariables = [
            "LOG_LEVEL": "DEBUG"
        ]
        let environment = LambdaClientTypes.Environment(variables: envVariables)

        do {
            let output = try await lambdaClient.updateFunctionConfiguration(
                input: UpdateFunctionConfigurationInput(
                    environment: environment,
                    functionName: functionName
                )
            )

            guard let response = output.environment else {
                throw ExampleError.environmentResponseMissingError
            }

            if response.error != nil {
                throw ExampleError.updateFunctionConfigurationError
            }

            guard let retVariables = response.variables else {
                throw ExampleError.environmentVariablesMissingError
            }

            for envVar in retVariables {
                if envVar.key == "LOG_LEVEL" && envVar.value != "DEBUG" {
                    print("*** Log level is not set to DEBUG!")
                    throw ExampleError.logLevelIncorrectError
                }
            }
        } catch {
            throw ExampleError.updateFunctionConfigurationError
        }
    }
```

- Pour plus de détails sur l'API, voir UpdateFunctionConfiguration dans AWS Référence du SDK pour l'API Swift.

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Scénarios pour Lambda utilisant AWS Kits SDK

Les exemples de code suivants vous montrent comment implémenter des scénarios courants dans Lambda avec AWS SDK. Ces scénarios vous montrent comment accomplir des tâches spécifiques en appelant plusieurs fonctions au sein de Lambda ou combinées avec d'autres Services AWS. Chaque exemple inclut un lien vers le code source complet, où vous trouverez des instructions sur la configuration et l'exécution du code.

Les scénarios ciblent un niveau d'expérience intermédiaire pour vous aider à comprendre les actions de service dans leur contexte.

Exemples

- Confirmez automatiquement les utilisateurs connus d'Amazon Cognito à l'aide d'une fonction Lambda à l'aide d'un AWS Kit SDK
- Migrez automatiquement les utilisateurs connus d'Amazon Cognito à l'aide d'une fonction Lambda à l'aide d'un AWS Kit SDK
- Créez une API REST API Gateway pour effectuer le suivi COVID-19 données
- Créer une API REST de bibliothèque de prêt
- Créer une application de messagerie avec Step Functions
- Création d'une API REST avec intégration de fonctions proxy
- Création d'une application de gestion des ressources photographiques permettant aux utilisateurs de gérer les photos à l'aide d'étiquettes
- Créer une application de chat Websocket avec API Gateway
- Créez une application qui analyse les commentaires des clients et synthétise le son
- Création d'un tableau de bord de surveillance avec le nom de fonction comme variable
- Création de votre première fonction sans serveur
- Invoquer une fonction Lambda à partir d'un navigateur
- Transformation des données pour votre application avec S3 Object Lambda
- Utiliser API Gateway pour invoquer une fonction Lambda
- Utiliser les fonctions Step Functions pour invoquer des fonctions Lambda

- Utilisent des événements planifiés pour invoquer une fonction Lambda
- Utiliser l'API Amazon Neptune pour développer une fonction Lambda qui interroge les données d'un graphe
- Utilisation de variables de propriété dans les tableaux de bord de surveillance pour surveiller plusieurs fonctions sans serveur
- Écrivez des données d'activité personnalisées à l'aide d'une fonction Lambda après l'authentification utilisateur Amazon Cognito à l'aide d'un AWS Kit SDK

Confirmez automatiquement les utilisateurs connus d'Amazon Cognito à l'aide d'une fonction Lambda à l'aide d'un AWS Kit SDK

Les exemples de code suivants illustrent comment confirmer automatiquement les utilisateurs Amazon Cognito connus avec une fonction Lambda.

- Configurez un groupe d'utilisateurs pour appeler une fonction Lambda pour le déclencheur `PreSignUp`.
- Inscription d'un utilisateur avec Amazon Cognito.
- La fonction Lambda analyse une table DynamoDB et confirme automatiquement les utilisateurs connus.
- Connectez-vous en tant que nouvel utilisateur, puis nettoyez les ressources.

Go

Kit SDK pour Go V2

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Exécutez un scénario interactif à une invite de commande.

```
import (
 "context"
```

```
 "errors"
 "log"
 "strings"
 "user_pools_and_lambda_triggers/actions"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/service/cognitoidentityprovider"
 "github.com/aws/aws-sdk-go-v2/service/cognitoidentityprovider/types"
 "github.com/awsdocs/aws-doc-sdk-examples/gov2/demotools"
)

// AutoConfirm separates the steps of this scenario into individual functions so
 that
// they are simpler to read and understand.
type AutoConfirm struct {
 helper       IScenarioHelper
 questioner   demotools.IQuestioner
 resources    Resources
 cognitoActor *actions.CognitoActions
}

// NewAutoConfirm constructs a new auto confirm runner.
func NewAutoConfirm(sdkConfig aws.Config, questioner demotools.IQuestioner,
 helper IScenarioHelper) AutoConfirm {
 scenario := AutoConfirm{
  helper:       helper,
  questioner:   questioner,
  resources:    Resources{},
  cognitoActor: &actions.CognitoActions{CognitoClient:
 cognitoidentityprovider.NewFromConfig(sdkConfig)},
 }
 scenario.resources.init(scenario.cognitoActor, questioner)
 return scenario
}

// AddPreSignUpTrigger adds a Lambda handler as an invocation target for the
 PreSignUp trigger.
func (runner *AutoConfirm) AddPreSignUpTrigger(ctx context.Context, userPoolId
 string, functionArn string) {
 log.Printf("Let's add a Lambda function to handle the PreSignUp trigger from
 Cognito.\n" +
  "This trigger happens when a user signs up, and lets your function take action
 before the main Cognito\n" +
  "sign up processing occurs.\n")
```

```
 err := runner.cognitoActor.UpdateTriggers(
  ctx, userPoolId,
  actions.TriggerInfo{Trigger: actions.PreSignUp, HandlerArn:
 aws.String(functionArn)})
 if err != nil {
  panic(err)
 }
 log.Printf("Lambda function %v added to user pool %v to handle the PreSignUp
 trigger.\n",
  functionArn, userPoolId)
}

// SignUpUser signs up a user from the known user table with a password you
 specify.
func (runner *AutoConfirm) SignUpUser(ctx context.Context, clientId string,
 usersTable string) (string, string) {
 log.Println("Let's sign up a user to your Cognito user pool. When the user's
 email matches an email in the\n" +
  "DynamoDB known users table, it is automatically verified and the user is
 confirmed.")

 knownUsers, err := runner.helper.GetKnownUsers(ctx, usersTable)
 if err != nil {
  panic(err)
 }
 userChoice := runner.questioner.AskChoice("Which user do you want to use?\n",
 knownUsers.UserNameList())
 user := knownUsers.Users[userChoice]

 var signedUp bool
 var userConfirmed bool
 password := runner.questioner.AskPassword("Enter a password that has at least
 eight characters, uppercase, lowercase, numbers and symbols.\n"+
  "(the password will not display as you type):", 8)
 for !signedUp {
  log.Printf("Signing up user '%v' with email '%v' to Cognito.\n", user.UserName,
 user.UserEmail)
  userConfirmed, err = runner.cognitoActor.SignUp(ctx, clientId, user.UserName,
 password, user.UserEmail)
  if err != nil {
   var invalidPassword *types.InvalidPasswordException
   if errors.As(err, &invalidPassword) {
    password = runner.questioner.AskPassword("Enter another password:", 8)
   } else {
```

```
    panic(err)
   }
  } else {
   signedUp = true
  }
 }
 log.Printf("User %v signed up, confirmed = %v.\n", user.UserName, userConfirmed)

 log.Println(strings.Repeat("-", 88))

 return user.UserName, password
}

// SignInUser signs in a user.
func (runner *AutoConfirm) SignInUser(ctx context.Context, clientId string,
 userName string, password string) string {
 runner.questioner.Ask("Press Enter when you're ready to continue.")
 log.Printf("Let's sign in as %v...\n", userName)
 authResult, err := runner.cognitoActor.SignIn(ctx, clientId, userName, password)
 if err != nil {
  panic(err)
 }
 log.Printf("Successfully signed in. Your access token starts with: %v...\n",
 (*authResult.AccessToken)[:10])
 log.Println(strings.Repeat("-", 88))
 return *authResult.AccessToken
}

// Run runs the scenario.
func (runner *AutoConfirm) Run(ctx context.Context, stackName string) {
 defer func() {
  if r := recover(); r != nil {
   log.Println("Something went wrong with the demo.")
   runner.resources.Cleanup(ctx)
  }
 }()

 log.Println(strings.Repeat("-", 88))
 log.Printf("Welcome\n")

 log.Println(strings.Repeat("-", 88))

 stackOutputs, err := runner.helper.GetStackOutputs(ctx, stackName)
 if err != nil {
```

```
  panic(err)
 }
 runner.resources.userPoolId = stackOutputs["UserPoolId"]
 runner.helper.PopulateUserTable(ctx, stackOutputs["TableName"])

 runner.AddPreSignUpTrigger(ctx, stackOutputs["UserPoolId"],
 stackOutputs["AutoConfirmFunctionArn"])
 runner.resources.triggers = append(runner.resources.triggers, actions.PreSignUp)
 userName, password := runner.SignUpUser(ctx, stackOutputs["UserPoolClientId"],
 stackOutputs["TableName"])
 runner.helper.ListRecentLogEvents(ctx, stackOutputs["AutoConfirmFunction"])
 runner.resources.userAccessTokens = append(runner.resources.userAccessTokens,
  runner.SignInUser(ctx, stackOutputs["UserPoolClientId"], userName, password))

 runner.resources.Cleanup(ctx)

 log.Println(strings.Repeat("-", 88))
 log.Println("Thanks for watching!")
 log.Println(strings.Repeat("-", 88))
}
```

Gérez le déclencheur `PreSignUp` avec une fonction Lambda.

```
import (
 "context"
 "log"
 "os"

 "github.com/aws/aws-lambda-go/events"
 "github.com/aws/aws-lambda-go/lambda"
 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/config"
 "github.com/aws/aws-sdk-go-v2/feature/dynamodb/attributevalue"
 "github.com/aws/aws-sdk-go-v2/service/dynamodb"
 dynamodbtypes "github.com/aws/aws-sdk-go-v2/service/dynamodb/types"
)

const TABLE_NAME = "TABLE_NAME"
```

```
// UserInfo defines structured user data that can be marshalled to a DynamoDB
 format.
type UserInfo struct {
 UserName  string `dynamodbav:"UserName"`
 UserEmail string `dynamodbav:"UserEmail"`
}

// GetKey marshals the user email value to a DynamoDB key format.
func (user UserInfo) GetKey() map[string]dynamodbtypes.AttributeValue {
 userEmail, err := attributevalue.Marshal(user.UserEmail)
 if err != nil {
  panic(err)
 }
 return map[string]dynamodbtypes.AttributeValue{"UserEmail": userEmail}
}

type handler struct {
 dynamoClient *dynamodb.Client
}

// HandleRequest handles the PreSignUp event by looking up a user in an Amazon
 DynamoDB table and
// specifying whether they should be confirmed and verified.
func (h *handler) HandleRequest(ctx context.Context, event
 events.CognitoEventUserPoolsPreSignup) (events.CognitoEventUserPoolsPreSignup,
 error) {
 log.Printf("Received presignup from %v for user '%v'", event.TriggerSource,
 event.UserName)
 if event.TriggerSource != "PreSignUp_SignUp" {
  // Other trigger sources, such as PreSignUp_AdminInitiateAuth, ignore the
 response from this handler.
  return event, nil
 }
 tableName := os.Getenv(TABLE_NAME)
 user := UserInfo{
  UserEmail: event.Request.UserAttributes["email"],
 }
 log.Printf("Looking up email %v in table %v.\n", user.UserEmail, tableName)
 output, err := h.dynamoClient.GetItem(ctx, &dynamodb.GetItemInput{
  Key:       user.GetKey(),
  TableName: aws.String(tableName),
 })
 if err != nil {
  log.Printf("Error looking up email %v.\n", user.UserEmail)
```

```
  return event, err
 }
 if output.Item == nil {
  log.Printf("Email %v not found. Email verification is required.\n",
 user.UserEmail)
  return event, err
 }

 err = attributevalue.UnmarshalMap(output.Item, &user)
 if err != nil {
  log.Printf("Couldn't unmarshal DynamoDB item. Here's why: %v\n", err)
  return event, err
 }

 if user.UserName != event.UserName {
  log.Printf("UserEmail %v found, but stored UserName '%v' does not match
 supplied UserName '%v'. Verification is required.\n",
   user.UserEmail, user.UserName, event.UserName)
 } else {
  log.Printf("UserEmail %v found with matching UserName %v. User is confirmed.
\n", user.UserEmail, user.UserName)
  event.Response.AutoConfirmUser = true
  event.Response.AutoVerifyEmail = true
 }

 return event, err
}

func main() {
 ctx := context.Background()
 sdkConfig, err := config.LoadDefaultConfig(ctx)
 if err != nil {
  log.Panicln(err)
 }
 h := handler{
  dynamoClient: dynamodb.NewFromConfig(sdkConfig),
 }
 lambda.Start(h.HandleRequest)
}
```

Créez une structure qui exécute les tâches courantes.

```
import (
 "context"
 "log"
 "strings"
 "time"
 "user_pools_and_lambda_triggers/actions"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/service/cloudformation"
 "github.com/aws/aws-sdk-go-v2/service/cloudwatchlogs"
 "github.com/aws/aws-sdk-go-v2/service/dynamodb"
 "github.com/awsdocs/aws-doc-sdk-examples/gov2/demotools"
)

// IScenarioHelper defines common functions used by the workflows in this
 example.
type IScenarioHelper interface {
 Pause(secs int)
 GetStackOutputs(ctx context.Context, stackName string) (actions.StackOutputs,
 error)
 PopulateUserTable(ctx context.Context, tableName string)
 GetKnownUsers(ctx context.Context, tableName string) (actions.UserList, error)
 AddKnownUser(ctx context.Context, tableName string, user actions.User)
 ListRecentLogEvents(ctx context.Context, functionName string)
}

// ScenarioHelper contains AWS wrapper structs used by the workflows in this
 example.
type ScenarioHelper struct {
 questioner  demotools.IQuestioner
 dynamoActor *actions.DynamoActions
 cfnActor    *actions.CloudFormationActions
 cwlActor    *actions.CloudWatchLogsActions
 isTestRun   bool
}

// NewScenarioHelper constructs a new scenario helper.
func NewScenarioHelper(sdkConfig aws.Config, questioner demotools.IQuestioner)
 ScenarioHelper {
 scenario := ScenarioHelper{
  questioner:  questioner,
```

```
  dynamoActor: &actions.DynamoActions{DynamoClient:
 dynamodb.NewFromConfig(sdkConfig)},
  cfnActor:    &actions.CloudFormationActions{CfnClient:
 cloudformation.NewFromConfig(sdkConfig)},
  cwlActor:    &actions.CloudWatchLogsActions{CwlClient:
 cloudwatchlogs.NewFromConfig(sdkConfig)},
 }
 return scenario
}

// Pause waits for the specified number of seconds.
func (helper ScenarioHelper) Pause(secs int) {
 if !helper.isTestRun {
  time.Sleep(time.Duration(secs) * time.Second)
 }
}

// GetStackOutputs gets the outputs from the specified CloudFormation stack in a
 structured format.
func (helper ScenarioHelper) GetStackOutputs(ctx context.Context, stackName
 string) (actions.StackOutputs, error) {
 return helper.cfnActor.GetOutputs(ctx, stackName), nil
}

// PopulateUserTable fills the known user table with example data.
func (helper ScenarioHelper) PopulateUserTable(ctx context.Context, tableName
 string) {
 log.Printf("First, let's add some users to the DynamoDB %v table we'll use for
 this example.\n", tableName)
 err := helper.dynamoActor.PopulateTable(ctx, tableName)
 if err != nil {
  panic(err)
 }
}

// GetKnownUsers gets the users from the known users table in a structured
 format.
func (helper ScenarioHelper) GetKnownUsers(ctx context.Context, tableName string)
 (actions.UserList, error) {
 knownUsers, err := helper.dynamoActor.Scan(ctx, tableName)
 if err != nil {
  log.Printf("Couldn't get known users from table %v. Here's why: %v\n",
 tableName, err)
 }
```

```
 return knownUsers, err
}

// AddKnownUser adds a user to the known users table.
func (helper ScenarioHelper) AddKnownUser(ctx context.Context, tableName string,
 user actions.User) {
 log.Printf("Adding user '%v' with email '%v' to the DynamoDB known users
 table...\n",
  user.UserName, user.UserEmail)
 err := helper.dynamoActor.AddUser(ctx, tableName, user)
 if err != nil {
  panic(err)
 }
}

// ListRecentLogEvents gets the most recent log stream and events for the
 specified Lambda function and displays them.
func (helper ScenarioHelper) ListRecentLogEvents(ctx context.Context,
 functionName string) {
 log.Println("Waiting a few seconds to let Lambda write to CloudWatch Logs...")
 helper.Pause(10)
 log.Println("Okay, let's check the logs to find what's happened recently with
 your Lambda function.")
 logStream, err := helper.cwlActor.GetLatestLogStream(ctx, functionName)
 if err != nil {
  panic(err)
 }
 log.Printf("Getting some recent events from log stream %v\n",
 *logStream.LogStreamName)
 events, err := helper.cwlActor.GetLogEvents(ctx, functionName,
 *logStream.LogStreamName, 10)
 if err != nil {
  panic(err)
 }
 for _, event := range events {
  log.Printf("\t%v", *event.Message)
 }
 log.Println(strings.Repeat("-", 88))
}
```

Créez une structure qui encapsule les actions Amazon Cognito.

```
import (
 "context"
 "errors"
 "log"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/service/cognitoidentityprovider"
 "github.com/aws/aws-sdk-go-v2/service/cognitoidentityprovider/types"
)

type CognitoActions struct {
 CognitoClient *cognitoidentityprovider.Client
}



// Trigger and TriggerInfo define typed data for updating an Amazon Cognito
 trigger.
type Trigger int

const (
 PreSignUp Trigger = iota
 UserMigration
 PostAuthentication
)

type TriggerInfo struct {
 Trigger    Trigger
 HandlerArn *string
}

// UpdateTriggers adds or removes Lambda triggers for a user pool. When a trigger
 is specified with a `nil` value,
// it is removed from the user pool.
func (actor CognitoActions) UpdateTriggers(ctx context.Context, userPoolId
 string, triggers ...TriggerInfo) error {
 output, err := actor.CognitoClient.DescribeUserPool(ctx,
 &cognitoidentityprovider.DescribeUserPoolInput{
  UserPoolId: aws.String(userPoolId),
 })
 if err != nil {
```

```
  log.Printf("Couldn't get info about user pool %v. Here's why: %v\n",
 userPoolId, err)
  return err
 }
 lambdaConfig := output.UserPool.LambdaConfig
 for _, trigger := range triggers {
  switch trigger.Trigger {
  case PreSignUp:
   lambdaConfig.PreSignUp = trigger.HandlerArn
  case UserMigration:
   lambdaConfig.UserMigration = trigger.HandlerArn
  case PostAuthentication:
   lambdaConfig.PostAuthentication = trigger.HandlerArn
  }
 }
 _, err = actor.CognitoClient.UpdateUserPool(ctx,
 &cognitoidentityprovider.UpdateUserPoolInput{
  UserPoolId:   aws.String(userPoolId),
  LambdaConfig: lambdaConfig,
 })
 if err != nil {
  log.Printf("Couldn't update user pool %v. Here's why: %v\n", userPoolId, err)
 }
 return err
}



// SignUp signs up a user with Amazon Cognito.
func (actor CognitoActions) SignUp(ctx context.Context, clientId string, userName
 string, password string, userEmail string) (bool, error) {
 confirmed := false
 output, err := actor.CognitoClient.SignUp(ctx,
 &cognitoidentityprovider.SignUpInput{
  ClientId: aws.String(clientId),
  Password: aws.String(password),
  Username: aws.String(userName),
  UserAttributes: []types.AttributeType{
   {Name: aws.String("email"), Value: aws.String(userEmail)},
  },
 })
 if err != nil {
  var invalidPassword *types.InvalidPasswordException
  if errors.As(err, &invalidPassword) {
```

```
   log.Println(*invalidPassword.Message)
  } else {
   log.Printf("Couldn't sign up user %v. Here's why: %v\n", userName, err)
  }
 } else {
  confirmed = output.UserConfirmed
 }
 return confirmed, err
}



// SignIn signs in a user to Amazon Cognito using a username and password
 authentication flow.
func (actor CognitoActions) SignIn(ctx context.Context, clientId string, userName
 string, password string) (*types.AuthenticationResultType, error) {
 var authResult *types.AuthenticationResultType
 output, err := actor.CognitoClient.InitiateAuth(ctx,
 &cognitoidentityprovider.InitiateAuthInput{
  AuthFlow:       "USER_PASSWORD_AUTH",
  ClientId:       aws.String(clientId),
  AuthParameters: map[string]string{"USERNAME": userName, "PASSWORD": password},
 })
 if err != nil {
  var resetRequired *types.PasswordResetRequiredException
  if errors.As(err, &resetRequired) {
   log.Println(*resetRequired.Message)
  } else {
   log.Printf("Couldn't sign in user %v. Here's why: %v\n", userName, err)
  }
 } else {
  authResult = output.AuthenticationResult
 }
 return authResult, err
}



// ForgotPassword starts a password recovery flow for a user. This flow typically
 sends a confirmation code
// to the user's configured notification destination, such as email.
func (actor CognitoActions) ForgotPassword(ctx context.Context, clientId string,
 userName string) (*types.CodeDeliveryDetailsType, error) {
```

```
 output, err := actor.CognitoClient.ForgotPassword(ctx,
 &cognitoidentityprovider.ForgotPasswordInput{
  ClientId: aws.String(clientId),
  Username: aws.String(userName),
 })
 if err != nil {
  log.Printf("Couldn't start password reset for user '%v'. Here;s why: %v\n",
 userName, err)
 }
 return output.CodeDeliveryDetails, err
}



// ConfirmForgotPassword confirms a user with a confirmation code and a new
 password.
func (actor CognitoActions) ConfirmForgotPassword(ctx context.Context, clientId
 string, code string, userName string, password string) error {
 _, err := actor.CognitoClient.ConfirmForgotPassword(ctx,
 &cognitoidentityprovider.ConfirmForgotPasswordInput{
  ClientId:         aws.String(clientId),
  ConfirmationCode: aws.String(code),
  Password:         aws.String(password),
  Username:         aws.String(userName),
 })
 if err != nil {
  var invalidPassword *types.InvalidPasswordException
  if errors.As(err, &invalidPassword) {
   log.Println(*invalidPassword.Message)
  } else {
   log.Printf("Couldn't confirm user %v. Here's why: %v", userName, err)
  }
 }
 return err
}



// DeleteUser removes a user from the user pool.
func (actor CognitoActions) DeleteUser(ctx context.Context, userAccessToken
 string) error {
 _, err := actor.CognitoClient.DeleteUser(ctx,
 &cognitoidentityprovider.DeleteUserInput{
  AccessToken: aws.String(userAccessToken),
```

```
 })
 if err != nil {
  log.Printf("Couldn't delete user. Here's why: %v\n", err)
 }
 return err
}



// AdminCreateUser uses administrator credentials to add a user to a user pool.
 This method leaves the user
// in a state that requires they enter a new password next time they sign in.
func (actor CognitoActions) AdminCreateUser(ctx context.Context, userPoolId
 string, userName string, userEmail string) error {
 _, err := actor.CognitoClient.AdminCreateUser(ctx,
 &cognitoidentityprovider.AdminCreateUserInput{
  UserPoolId:     aws.String(userPoolId),
  Username:       aws.String(userName),
  MessageAction:  types.MessageActionTypeSuppress,
  UserAttributes: []types.AttributeType{{Name: aws.String("email"), Value:
 aws.String(userEmail)}},
 })
 if err != nil {
  var userExists *types.UsernameExistsException
  if errors.As(err, &userExists) {
   log.Printf("User %v already exists in the user pool.", userName)
   err = nil
  } else {
   log.Printf("Couldn't create user %v. Here's why: %v\n", userName, err)
  }
 }
 return err
}



// AdminSetUserPassword uses administrator credentials to set a password for a
 user without requiring a
// temporary password.
func (actor CognitoActions) AdminSetUserPassword(ctx context.Context, userPoolId
 string, userName string, password string) error {
 _, err := actor.CognitoClient.AdminSetUserPassword(ctx,
 &cognitoidentityprovider.AdminSetUserPasswordInput{
  Password:   aws.String(password),
```

```
  UserPoolId: aws.String(userPoolId),
  Username:   aws.String(userName),
  Permanent:  true,
 })
 if err != nil {
  var invalidPassword *types.InvalidPasswordException
  if errors.As(err, &invalidPassword) {
   log.Println(*invalidPassword.Message)
  } else {
   log.Printf("Couldn't set password for user %v. Here's why: %v\n", userName,
 err)
  }
 }
 return err
}
```

Créez une structure qui encapsule les actions DynamoDB.

```
import (
 "context"
 "fmt"
 "log"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/feature/dynamodb/attributevalue"
 "github.com/aws/aws-sdk-go-v2/service/dynamodb"
 "github.com/aws/aws-sdk-go-v2/service/dynamodb/types"
)

// DynamoActions encapsulates the Amazon Simple Notification Service (Amazon SNS)
 actions
// used in the examples.
type DynamoActions struct {
 DynamoClient *dynamodb.Client
}

// User defines structured user data.
type User struct {
 UserName  string
 UserEmail string
```

```
 LastLogin *LoginInfo `dynamodbav:",omitempty"`
}

// LoginInfo defines structured custom login data.
type LoginInfo struct {
 UserPoolId string
 ClientId   string
 Time       string
}

// UserList defines a list of users.
type UserList struct {
 Users []User
}

// UserNameList returns the usernames contained in a UserList as a list of
 strings.
func (users *UserList) UserNameList() []string {
 names := make([]string, len(users.Users))
 for i := 0; i < len(users.Users); i++ {
  names[i] = users.Users[i].UserName
 }
 return names
}

// PopulateTable adds a set of test users to the table.
func (actor DynamoActions) PopulateTable(ctx context.Context, tableName string)
 error {
 var err error
 var item map[string]types.AttributeValue
 var writeReqs []types.WriteRequest
 for i := 1; i < 4; i++ {
  item, err = attributevalue.MarshalMap(User{UserName: fmt.Sprintf("test_user_
%v", i), UserEmail: fmt.Sprintf("test_email_%v@example.com", i)})
  if err != nil {
   log.Printf("Couldn't marshall user into DynamoDB format. Here's why: %v\n",
 err)
   return err
  }
  writeReqs = append(writeReqs, types.WriteRequest{PutRequest:
 &types.PutRequest{Item: item}})
 }
 _, err = actor.DynamoClient.BatchWriteItem(ctx, &dynamodb.BatchWriteItemInput{
  RequestItems: map[string][]types.WriteRequest{tableName: writeReqs},
```

```
 })
 if err != nil {
  log.Printf("Couldn't populate table %v with users. Here's why: %v\n",
 tableName, err)
 }
 return err
}

// Scan scans the table for all items.
func (actor DynamoActions) Scan(ctx context.Context, tableName string) (UserList,
 error) {
 var userList UserList
 output, err := actor.DynamoClient.Scan(ctx, &dynamodb.ScanInput{
  TableName: aws.String(tableName),
 })
 if err != nil {
  log.Printf("Couldn't scan table %v for items. Here's why: %v\n", tableName,
 err)
 } else {
  err = attributevalue.UnmarshalListOfMaps(output.Items, &userList.Users)
  if err != nil {
   log.Printf("Couldn't unmarshal items into users. Here's why: %v\n", err)
  }
 }
 return userList, err
}

// AddUser adds a user item to a table.
func (actor DynamoActions) AddUser(ctx context.Context, tableName string, user
 User) error {
 userItem, err := attributevalue.MarshalMap(user)
 if err != nil {
  log.Printf("Couldn't marshall user to item. Here's why: %v\n", err)
 }
 _, err = actor.DynamoClient.PutItem(ctx, &dynamodb.PutItemInput{
  Item:      userItem,
  TableName: aws.String(tableName),
 })
 if err != nil {
  log.Printf("Couldn't put item in table %v. Here's why: %v", tableName, err)
 }
 return err
}
```

Créez une structure qui enveloppe CloudWatch Enregistre les actions.

```
import (
 "context"
 "fmt"
 "log"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/service/cloudwatchlogs"
 "github.com/aws/aws-sdk-go-v2/service/cloudwatchlogs/types"
)

type CloudWatchLogsActions struct {
 CwlClient *cloudwatchlogs.Client
}

// GetLatestLogStream gets the most recent log stream for a Lambda function.
func (actor CloudWatchLogsActions) GetLatestLogStream(ctx context.Context,
 functionName string) (types.LogStream, error) {
 var logStream types.LogStream
 logGroupName := fmt.Sprintf("/aws/lambda/%s", functionName)
 output, err := actor.CwlClient.DescribeLogStreams(ctx,
 &cloudwatchlogs.DescribeLogStreamsInput{
  Descending:   aws.Bool(true),
  Limit:        aws.Int32(1),
  LogGroupName: aws.String(logGroupName),
  OrderBy:      types.OrderByLastEventTime,
 })
 if err != nil {
  log.Printf("Couldn't get log streams for log group %v. Here's why: %v\n",
 logGroupName, err)
 } else {
  logStream = output.LogStreams[0]
 }
 return logStream, err
}

// GetLogEvents gets the most recent eventCount events from the specified log
 stream.
```

```
func (actor CloudWatchLogsActions) GetLogEvents(ctx context.Context, functionName
 string, logStreamName string, eventCount int32) (
 []types.OutputLogEvent, error) {
 var events []types.OutputLogEvent
 logGroupName := fmt.Sprintf("/aws/lambda/%s", functionName)
 output, err := actor.CwlClient.GetLogEvents(ctx,
 &cloudwatchlogs.GetLogEventsInput{
  LogStreamName: aws.String(logStreamName),
  Limit:         aws.Int32(eventCount),
  LogGroupName:  aws.String(logGroupName),
 })
 if err != nil {
  log.Printf("Couldn't get log event for log stream %v. Here's why: %v\n",
 logStreamName, err)
 } else {
  events = output.Events
 }
 return events, err
}
```

Créez une structure qui enveloppe CloudFormation actions.

```
import (
 "context"
 "log"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/service/cloudformation"
)

// StackOutputs defines a map of outputs from a specific stack.
type StackOutputs map[string]string

type CloudFormationActions struct {
 CfnClient *cloudformation.Client
}

// GetOutputs gets the outputs from a CloudFormation stack and puts them into a
 structured format.
```

```
func (actor CloudFormationActions) GetOutputs(ctx context.Context, stackName
 string) StackOutputs {
 output, err := actor.CfnClient.DescribeStacks(ctx,
 &cloudformation.DescribeStacksInput{
  StackName: aws.String(stackName),
 })
 if err != nil || len(output.Stacks) == 0 {
  log.Panicf("Couldn't find a CloudFormation stack named %v. Here's why: %v\n",
 stackName, err)
 }
 stackOutputs := StackOutputs{}
 for _, out := range output.Stacks[0].Outputs {
  stackOutputs[*out.OutputKey] = *out.OutputValue
 }
 return stackOutputs
}
```

Nettoyez les ressources.

```
import (
 "context"
 "log"
 "user_pools_and_lambda_triggers/actions"

 "github.com/awsdocs/aws-doc-sdk-examples/gov2/demotools"
)

// Resources keeps track of AWS resources created during an example and handles
// cleanup when the example finishes.
type Resources struct {
 userPoolId       string
 userAccessTokens []string
 triggers         []actions.Trigger

 cognitoActor *actions.CognitoActions
 questioner   demotools.IQuestioner
}

func (resources *Resources) init(cognitoActor *actions.CognitoActions, questioner
 demotools.IQuestioner) {
```

```
 resources.userAccessTokens = []string{}
 resources.triggers = []actions.Trigger{}
 resources.cognitoActor = cognitoActor
 resources.questioner = questioner
}

// Cleanup deletes all AWS resources created during an example.
func (resources *Resources) Cleanup(ctx context.Context) {
 defer func() {
  if r := recover(); r != nil {
   log.Printf("Something went wrong during cleanup.\n%v\n", r)
   log.Println("Use the AWS Management Console to remove any remaining resources
 \n" +
    "that were created for this scenario.")
  }
 }()

 wantDelete := resources.questioner.AskBool("Do you want to remove all of the AWS
 resources that were created "+
  "during this demo (y/n)?", "y")
 if wantDelete {
  for _, accessToken := range resources.userAccessTokens {
   err := resources.cognitoActor.DeleteUser(ctx, accessToken)
   if err != nil {
    log.Println("Couldn't delete user during cleanup.")
    panic(err)
   }
   log.Println("Deleted user.")
  }
  triggerList := make([]actions.TriggerInfo, len(resources.triggers))
  for i := 0; i < len(resources.triggers); i++ {
   triggerList[i] = actions.TriggerInfo{Trigger: resources.triggers[i],
 HandlerArn: nil}
  }
  err := resources.cognitoActor.UpdateTriggers(ctx, resources.userPoolId,
 triggerList...)
  if err != nil {
   log.Println("Couldn't update Cognito triggers during cleanup.")
   panic(err)
  }
  log.Println("Removed Cognito triggers from user pool.")
 } else {
  log.Println("Be sure to remove resources when you're done with them to avoid
 unexpected charges!")
```

```
 }
}
```

- Pour plus de détails sur l'API, consultez les rubriques suivantes dans la Référence des API du kit AWS SDK pour Go .
  - DeleteUser
  - InitiateAuth
  - SignUp
  - UpdateUserPool

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Configurez une exécution interactive de type « Scénario ». Le JavaScript Les exemples (v3) partagent un Scenario Runner pour rationaliser les exemples complexes. Le code source complet est activé GitHub.

```
import { AutoConfirm } from "./scenario-auto-confirm.js";

/**
 * The context is passed to every scenario. Scenario steps
 * will modify the context.
 */
const context = {
  errors: [],
  users: [
    {
      UserName: "test_user_1",
      UserEmail: "test_email_1@example.com",
    },
```

```
    {
      UserName: "test_user_2",
      UserEmail: "test_email_2@example.com",
    },
    {
      UserName: "test_user_3",
      UserEmail: "test_email_3@example.com",
    },
  ],
};

/**
 * Three Scenarios are created for the workflow. A Scenario is an orchestration
 class
 * that simplifies running a series of steps.
 */
export const scenarios = {
  // Demonstrate automatically confirming known users in a database.
  "auto-confirm": AutoConfirm(context),
};

// Call function if run directly
import { fileURLToPath } from "node:url";
import { parseScenarioArgs } from "@aws-doc-sdk-examples/lib/scenario/index.js";

if (process.argv[1] === fileURLToPath(import.meta.url)) {
  parseScenarioArgs(scenarios, {
    name: "Cognito user pools and triggers",
    description:
      "Demonstrate how to use the AWS SDKs to customize Amazon Cognito
 authentication behavior.",
  });
}
```

Ce scénario illustre la confirmation automatique d'un utilisateur connu. Il orchestre les étapes de l'exemple.

```
import { wait } from "@aws-doc-sdk-examples/lib/utils/util-timers.js";
import {
  Scenario,
  ScenarioAction,
  ScenarioInput,
```

```
  ScenarioOutput,
} from "@aws-doc-sdk-examples/lib/scenario/scenario.js";

import {
  getStackOutputs,
  logCleanUpReminder,
  promptForStackName,
  promptForStackRegion,
  skipWhenErrors,
} from "./steps-common.js";
import { populateTable } from "./actions/dynamodb-actions.js";
import {
  addPreSignUpHandler,
  deleteUser,
  getUser,
  signIn,
  signUpUser,
} from "./actions/cognito-actions.js";
import {
  getLatestLogStreamForLambda,
  getLogEvents,
} from "./actions/cloudwatch-logs-actions.js";

/**
 * @typedef {{
 *   errors: Error[],
 *   password: string,
 *   users: { UserName: string, UserEmail: string }[],
 *   selectedUser?: string,
 *   stackName?: string,
 *   stackRegion?: string,
 *   token?: string,
 *   confirmDeleteSignedInUser?: boolean,
 *   TableName?: string,
 *   UserPoolClientId?: string,
 *   UserPoolId?: string,
 *   UserPoolArn?: string,
 *   AutoConfirmHandlerArn?: string,
 *   AutoConfirmHandlerName?: string
 * }} State
 */

const greeting = new ScenarioOutput(
  "greeting",
```

```
  (/** @type {State} */ state) => `This demo will populate some users into the \
database created as part of the "${state.stackName}" stack. \
Then the AutoConfirmHandler will be linked to the PreSignUp \
trigger from Cognito. Finally, you will choose a user to sign up.`,
  { skipWhen: skipWhenErrors },
);

const logPopulatingUsers = new ScenarioOutput(
  "logPopulatingUsers",
  "Populating the DynamoDB table with some users.",
  { skipWhenErrors: skipWhenErrors },
);

const logPopulatingUsersComplete = new ScenarioOutput(
  "logPopulatingUsersComplete",
  "Done populating users.",
  { skipWhen: skipWhenErrors },
);

const populateUsers = new ScenarioAction(
  "populateUsers",
  async (/** @type {State} */ state) => {
    const [_, err] = await populateTable({
      region: state.stackRegion,
      tableName: state.TableName,
      items: state.users,
    });
    if (err) {
      state.errors.push(err);
    }
  },
  {
    skipWhen: skipWhenErrors,
  },
);

const logSetupSignUpTrigger = new ScenarioOutput(
  "logSetupSignUpTrigger",
  "Setting up the PreSignUp trigger for the Cognito User Pool.",
  { skipWhen: skipWhenErrors },
);

const setupSignUpTrigger = new ScenarioAction(
  "setupSignUpTrigger",
```

```
  async (/** @type {State} */ state) => {
    const [_, err] = await addPreSignUpHandler({
      region: state.stackRegion,
      userPoolId: state.UserPoolId,
      handlerArn: state.AutoConfirmHandlerArn,
    });
    if (err) {
      state.errors.push(err);
    }
  },
  {
    skipWhen: skipWhenErrors,
  },
);

const logSetupSignUpTriggerComplete = new ScenarioOutput(
  "logSetupSignUpTriggerComplete",
  (
    /** @type {State} */ state,
  ) => `The lambda function "${state.AutoConfirmHandlerName}" \
has been configured as the PreSignUp trigger handler for the user pool
 "${state.UserPoolId}".`,
  { skipWhen: skipWhenErrors },
);

const selectUser = new ScenarioInput(
  "selectedUser",
  "Select a user to sign up.",
  {
    type: "select",
    choices: (/** @type {State} */ state) => state.users.map((u) => u.UserName),
    skipWhen: skipWhenErrors,
    default: (/** @type {State} */ state) => state.users[0].UserName,
  },
);

const checkIfUserAlreadyExists = new ScenarioAction(
  "checkIfUserAlreadyExists",
  async (/** @type {State} */ state) => {
    const [user, err] = await getUser({
      region: state.stackRegion,
      userPoolId: state.UserPoolId,
      username: state.selectedUser,
    });
```

```
    if (err?.name === "UserNotFoundException") {
      // Do nothing. We're not expecting the user to exist before
      // sign up is complete.
      return;
    }

    if (err) {
      state.errors.push(err);
      return;
    }

    if (user) {
      state.errors.push(
        new Error(
          `The user "${state.selectedUser}" already exists in the user pool
 "${state.UserPoolId}".`,
        ),
      );
    }
  },
  {
    skipWhen: skipWhenErrors,
  },
);

const createPassword = new ScenarioInput(
  "password",
  "Enter a password that has at least eight characters, uppercase, lowercase,
 numbers and symbols.",
  { type: "password", skipWhen: skipWhenErrors, default: "Abcd1234!" },
);

const logSignUpExistingUser = new ScenarioOutput(
  "logSignUpExistingUser",
  (/** @type {State} */ state) => `Signing up user "${state.selectedUser}".`,
  { skipWhen: skipWhenErrors },
);

const signUpExistingUser = new ScenarioAction(
  "signUpExistingUser",
  async (/** @type {State} */ state) => {
    const signUp = (password) =>
      signUpUser({
```

```
        region: state.stackRegion,
        userPoolClientId: state.UserPoolClientId,
        username: state.selectedUser,
        email: state.users.find((u) => u.UserName === state.selectedUser)
          .UserEmail,
        password,
      });

    let [_, err] = await signUp(state.password);

    while (err?.name === "InvalidPasswordException") {
      console.warn("The password you entered was invalid.");
      await createPassword.handle(state);
      [_, err] = await signUp(state.password);
    }

    if (err) {
      state.errors.push(err);
    }
  },
  { skipWhen: skipWhenErrors },
);

const logSignUpExistingUserComplete = new ScenarioOutput(
  "logSignUpExistingUserComplete",
  (/** @type {State} */ state) =>
    `"${state.selectedUser} was signed up successfully.`,
  { skipWhen: skipWhenErrors },
);

const logLambdaLogs = new ScenarioAction(
  "logLambdaLogs",
  async (/** @type {State} */ state) => {
    console.log(
      "Waiting a few seconds to let Lambda write to CloudWatch Logs...\n",
    );
    await wait(10);

    const [logStream, logStreamErr] = await getLatestLogStreamForLambda({
      functionName: state.AutoConfirmHandlerName,
      region: state.stackRegion,
    });
    if (logStreamErr) {
      state.errors.push(logStreamErr);
```

```
      return;
    }

    console.log(
      `Getting some recent events from log stream "${logStream.logStreamName}"`,
    );
    const [logEvents, logEventsErr] = await getLogEvents({
      functionName: state.AutoConfirmHandlerName,
      region: state.stackRegion,
      eventCount: 10,
      logStreamName: logStream.logStreamName,
    });
    if (logEventsErr) {
      state.errors.push(logEventsErr);
      return;
    }

    console.log(logEvents.map((ev) => `\t${ev.message}`).join(""));
  },
  { skipWhen: skipWhenErrors },
);

const logSignInUser = new ScenarioOutput(
  "logSignInUser",
  (/** @type {State} */ state) => `Let's sign in as ${state.selectedUser}`,
  { skipWhen: skipWhenErrors },
);

const signInUser = new ScenarioAction(
  "signInUser",
  async (/** @type {State} */ state) => {
    const [response, err] = await signIn({
      region: state.stackRegion,
      clientId: state.UserPoolClientId,
      username: state.selectedUser,
      password: state.password,
    });

    if (err?.name === "PasswordResetRequiredException") {
      state.errors.push(new Error("Please reset your password."));
      return;
    }

    if (err) {
```

```
      state.errors.push(err);
      return;
    }

    state.token = response?.AuthenticationResult?.AccessToken;
  },
  { skipWhen: skipWhenErrors },
);

const logSignInUserComplete = new ScenarioOutput(
  "logSignInUserComplete",
  (/** @type {State} */ state) =>
    `Successfully signed in. Your access token starts with:
 ${state.token.slice(0, 11)}`,
  { skipWhen: skipWhenErrors },
);

const confirmDeleteSignedInUser = new ScenarioInput(
  "confirmDeleteSignedInUser",
  "Do you want to delete the currently signed in user?",
  { type: "confirm", skipWhen: skipWhenErrors },
);

const deleteSignedInUser = new ScenarioAction(
  "deleteSignedInUser",
  async (/** @type {State} */ state) => {
    const [_, err] = await deleteUser({
      region: state.stackRegion,
      accessToken: state.token,
    });

    if (err) {
      state.errors.push(err);
    }
  },
  {
    skipWhen: (/** @type {State} */ state) =>
      skipWhenErrors(state) || !state.confirmDeleteSignedInUser,
  },
);

const logErrors = new ScenarioOutput(
  "logErrors",
  (/** @type {State}*/ state) => {
```

```
    const errorList = state.errors
      .map((err) => ` - ${err.name}: ${err.message}`)
      .join("\n");
    return `Scenario errors found:\n${errorList}`;
  },
  {
    // Don't log errors when there aren't any!
    skipWhen: (/** @type {State} */ state) => state.errors.length === 0,
  },
);

export const AutoConfirm = (context) =>
  new Scenario(
    "AutoConfirm",
    [
      promptForStackName,
      promptForStackRegion,
      getStackOutputs,
      greeting,
      logPopulatingUsers,
      populateUsers,
      logPopulatingUsersComplete,
      logSetupSignUpTrigger,
      setupSignUpTrigger,
      logSetupSignUpTriggerComplete,
      selectUser,
      checkIfUserAlreadyExists,
      createPassword,
      logSignUpExistingUser,
      signUpExistingUser,
      logSignUpExistingUserComplete,
      logLambdaLogs,
      logSignInUser,
      signInUser,
      logSignInUserComplete,
      confirmDeleteSignedInUser,
      deleteSignedInUser,
      logCleanUpReminder,
      logErrors,
    ],
    context,
  );
```

Ces étapes sont partagées avec d'autres scénarios.

```
import {
  ScenarioAction,
  ScenarioInput,
  ScenarioOutput,
} from "@aws-doc-sdk-examples/lib/scenario/scenario.js";
import { getCfnOutputs } from "@aws-doc-sdk-examples/lib/sdk/cfn-outputs.js";

export const skipWhenErrors = (state) => state.errors.length > 0;

export const getStackOutputs = new ScenarioAction(
  "getStackOutputs",
  async (state) => {
    if (!state.stackName || !state.stackRegion) {
      state.errors.push(
        new Error(
          "No stack name or region provided. The stack name and \
region are required to fetch CFN outputs relevant to this example.",
        ),
      );
      return;
    }

    const outputs = await getCfnOutputs(state.stackName, state.stackRegion);
    Object.assign(state, outputs);
  },
);

export const promptForStackName = new ScenarioInput(
  "stackName",
  "Enter the name of the stack you deployed earlier.",
  { type: "input", default: "PoolsAndTriggersStack" },
);

export const promptForStackRegion = new ScenarioInput(
  "stackRegion",
  "Enter the region of the stack you deployed earlier.",
  { type: "input", default: "us-east-1" },
);

export const logCleanUpReminder = new ScenarioOutput(
  "logCleanUpReminder",
  "All done. Remember to run 'cdk destroy' to teardown the stack.",
```

```
  { skipWhen: skipWhenErrors },
);
```

Un gestionnaire pour le déclencheur `PreSignUp` avec une fonction Lambda.

```
import type { PreSignUpTriggerEvent, Handler } from "aws-lambda";
import type { UserRepository } from "./user-repository";
import { DynamoDBUserRepository } from "./user-repository";

export class PreSignUpHandler {
  private userRepository: UserRepository;

  constructor(userRepository: UserRepository) {
    this.userRepository = userRepository;
  }

  private isPreSignUpTriggerSource(event: PreSignUpTriggerEvent): boolean {
    return event.triggerSource === "PreSignUp_SignUp";
  }

  private getEventUserEmail(event: PreSignUpTriggerEvent): string {
    return event.request.userAttributes.email;
  }

  async handlePreSignUpTriggerEvent(
    event: PreSignUpTriggerEvent,
  ): Promise<PreSignUpTriggerEvent> {
    console.log(
      `Received presignup from ${event.triggerSource} for user
 '${event.userName}'`,
    );

    if (!this.isPreSignUpTriggerSource(event)) {
      return event;
    }

    const eventEmail = this.getEventUserEmail(event);
    console.log(`Looking up email ${eventEmail}.`);
    const storedUserInfo =
      await this.userRepository.getUserInfoByEmail(eventEmail);

    if (!storedUserInfo) {
```

```
      console.log(
        `Email ${eventEmail} not found. Email verification is required.`,
      );
      return event;
    }

    if (storedUserInfo.UserName !== event.userName) {
      console.log(
        `UserEmail ${eventEmail} found, but stored UserName
 '${storedUserInfo.UserName}' does not match supplied UserName
 '${event.userName}'. Verification is required.`,
      );
    } else {
      console.log(
        `UserEmail ${eventEmail} found with matching UserName
 ${storedUserInfo.UserName}. User is confirmed.`,
      );
      event.response.autoConfirmUser = true;
      event.response.autoVerifyEmail = true;
    }
    return event;
  }
}

const createPreSignUpHandler = (): PreSignUpHandler => {
  const tableName = process.env.TABLE_NAME;
  if (!tableName) {
    throw new Error("TABLE_NAME environment variable is not set");
  }

  const userRepository = new DynamoDBUserRepository(tableName);
  return new PreSignUpHandler(userRepository);
};

export const handler: Handler = async (event: PreSignUpTriggerEvent) => {
  const preSignUpHandler = createPreSignUpHandler();
  return preSignUpHandler.handlePreSignUpTriggerEvent(event);
};
```

Module de CloudWatch Enregistre les actions.

```
import {
  CloudWatchLogsClient,
  GetLogEventsCommand,
  OrderBy,
  paginateDescribeLogStreams,
} from "@aws-sdk/client-cloudwatch-logs";

/**
 * Get the latest log stream for a Lambda function.
 * @param {{ functionName: string, region: string }} config
 * @returns {Promise<[import("@aws-sdk/client-cloudwatch-logs").LogStream | null,
 unknown]>}
 */
export const getLatestLogStreamForLambda = async ({ functionName, region }) => {
  try {
    const logGroupName = `/aws/lambda/${functionName}`;
    const cwlClient = new CloudWatchLogsClient({ region });
    const paginator = paginateDescribeLogStreams(
      { client: cwlClient },
      {
        descending: true,
        limit: 1,
        orderBy: OrderBy.LastEventTime,
        logGroupName,
      },
    );

    for await (const page of paginator) {
      return [page.logStreams[0], null];
    }
  } catch (err) {
    return [null, err];
  }
};

/**
 * Get the log events for a Lambda function's log stream.
 * @param {{
 *   functionName: string,
 *   logStreamName: string,
 *   eventCount: number,
 *   region: string
 * }} config
```

```
 * @returns {Promise<[import("@aws-sdk/client-cloudwatch-logs").OutputLogEvent[]
 | null, unknown]>}
 */
export const getLogEvents = async ({
  functionName,
  logStreamName,
  eventCount,
  region,
}) => {
  try {
    const cwlClient = new CloudWatchLogsClient({ region });
    const logGroupName = `/aws/lambda/${functionName}`;
    const response = await cwlClient.send(
      new GetLogEventsCommand({
        logStreamName: logStreamName,
        limit: eventCount,
        logGroupName: logGroupName,
      }),
    );

    return [response.events, null];
  } catch (err) {
    return [null, err];
  }
};
```

Module d’actions Amazon Cognito.

```
import {
  AdminGetUserCommand,
  CognitoIdentityProviderClient,
  DeleteUserCommand,
  InitiateAuthCommand,
  SignUpCommand,
  UpdateUserPoolCommand,
} from "@aws-sdk/client-cognito-identity-provider";

/**
 * Connect a Lambda function to the PreSignUp trigger for a Cognito user pool
 * @param {{ region: string, userPoolId: string, handlerArn: string }} config
```

```
 * @returns {Promise<[import("@aws-sdk/client-cognito-identity-
provider").UpdateUserPoolCommandOutput | null, unknown]>}
 */
export const addPreSignUpHandler = async ({
  region,
  userPoolId,
  handlerArn,
}) => {
  try {
    const cognitoClient = new CognitoIdentityProviderClient({
      region,
    });

    const command = new UpdateUserPoolCommand({
      UserPoolId: userPoolId,
      LambdaConfig: {
        PreSignUp: handlerArn,
      },
    });

    const response = await cognitoClient.send(command);
    return [response, null];
  } catch (err) {
    return [null, err];
  }
};

/**
 * Attempt to register a user to a user pool with a given username and password.
 * @param {{
 *   region: string,
 *   userPoolClientId: string,
 *   username: string,
 *   email: string,
 *   password: string
 * }} config
 * @returns {Promise<[import("@aws-sdk/client-cognito-identity-
provider").SignUpCommandOutput | null, unknown]>}
 */
export const signUpUser = async ({
  region,
  userPoolClientId,
  username,
  email,
```

```
  password,
}) => {
  try {
    const cognitoClient = new CognitoIdentityProviderClient({
      region,
    });

    const response = await cognitoClient.send(
      new SignUpCommand({
        ClientId: userPoolClientId,
        Username: username,
        Password: password,
        UserAttributes: [{ Name: "email", Value: email }],
      }),
    );
    return [response, null];
  } catch (err) {
    return [null, err];
  }
};

/**
 * Sign in a user to Amazon Cognito using a username and password authentication
 flow.
 * @param {{ region: string, clientId: string, username: string, password:
 string }} config
 * @returns {Promise<[import("@aws-sdk/client-cognito-identity-
provider").InitiateAuthCommandOutput | null, unknown]>}
 */
export const signIn = async ({ region, clientId, username, password }) => {
  try {
    const cognitoClient = new CognitoIdentityProviderClient({ region });
    const response = await cognitoClient.send(
      new InitiateAuthCommand({
        AuthFlow: "USER_PASSWORD_AUTH",
        ClientId: clientId,
        AuthParameters: { USERNAME: username, PASSWORD: password },
      }),
    );
    return [response, null];
  } catch (err) {
    return [null, err];
  }
};
```

```
/**
 * Retrieve an existing user from a user pool.
 * @param {{ region: string, userPoolId: string, username: string }} config
 * @returns {Promise<[import("@aws-sdk/client-cognito-identity-
provider").AdminGetUserCommandOutput | null, unknown]>}
 */
export const getUser = async ({ region, userPoolId, username }) => {
  try {
    const cognitoClient = new CognitoIdentityProviderClient({ region });
    const response = await cognitoClient.send(
      new AdminGetUserCommand({
        UserPoolId: userPoolId,
        Username: username,
      }),
    );
    return [response, null];
  } catch (err) {
    return [null, err];
  }
};

/**
 * Delete the signed-in user. Useful for allowing a user to delete their
 * own profile.
 * @param {{ region: string, accessToken: string }} config
 * @returns {Promise<[import("@aws-sdk/client-cognito-identity-
provider").DeleteUserCommandOutput | null, unknown]>}
 */
export const deleteUser = async ({ region, accessToken }) => {
  try {
    const client = new CognitoIdentityProviderClient({ region });
    const response = await client.send(
      new DeleteUserCommand({ AccessToken: accessToken }),
    );
    return [response, null];
  } catch (err) {
    return [null, err];
  }
};
```

Module d’actions DynamoDB.

```
import { DynamoDBClient } from "@aws-sdk/client-dynamodb";
import {
  BatchWriteCommand,
  DynamoDBDocumentClient,
} from "@aws-sdk/lib-dynamodb";

/**
 * Populate a DynamoDB table with provide items.
 * @param {{ region: string, tableName: string, items: Record<string,
 unknown>[] }} config
 * @returns {Promise<[import("@aws-sdk/lib-dynamodb").BatchWriteCommandOutput |
 null, unknown]>}
 */
export const populateTable = async ({ region, tableName, items }) => {
  try {
    const ddbClient = new DynamoDBClient({ region });
    const docClient = DynamoDBDocumentClient.from(ddbClient);
    const response = await docClient.send(
      new BatchWriteCommand({
        RequestItems: {
          [tableName]: items.map((item) => ({
            PutRequest: {
              Item: item,
            },
          })),
        },
      }),
    );
    return [response, null];
  } catch (err) {
    return [null, err];
  }
};
```

- Pour plus de détails sur l'API, consultez les rubriques suivantes dans la Référence des API du kit AWS SDK pour JavaScript .
  - DeleteUser
  - InitiateAuth
  - SignUp

- UpdateUserPool

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Migrez automatiquement les utilisateurs connus d'Amazon Cognito à l'aide d'une fonction Lambda à l'aide d'un AWS Kit SDK

L'exemple de code suivant illustre comment effectuer automatiquement une migration des utilisateurs Amazon Cognito connus avec une fonction Lambda.

- Configurez un groupe d'utilisateurs pour appeler une fonction Lambda pour le déclencheur `MigrateUser`.
- Connectez-vous à Amazon Cognito avec un nom d'utilisateur et une adresse e-mail qui ne figurent pas dans le groupe d'utilisateurs.
- La fonction Lambda analyse une table DynamoDB et transfère automatiquement les utilisateurs connus vers le groupe d'utilisateurs.
- Exécutez le flux de mots de passe oubliés pour réinitialiser le mot de passe de l'utilisateur soumis à la migration.
- Connectez-vous en tant que nouvel utilisateur, puis nettoyez les ressources.

Go

Kit SDK pour Go V2

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Exécutez un scénario interactif à une invite de commande.

```
import (
 "context"
```

```
 "errors"
 "fmt"
 "log"
 "strings"
 "user_pools_and_lambda_triggers/actions"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/service/cognitoidentityprovider"
 "github.com/aws/aws-sdk-go-v2/service/cognitoidentityprovider/types"
 "github.com/awsdocs/aws-doc-sdk-examples/gov2/demotools"
)

// MigrateUser separates the steps of this scenario into individual functions so
 that
// they are simpler to read and understand.
type MigrateUser struct {
 helper       IScenarioHelper
 questioner   demotools.IQuestioner
 resources    Resources
 cognitoActor *actions.CognitoActions
}

// NewMigrateUser constructs a new migrate user runner.
func NewMigrateUser(sdkConfig aws.Config, questioner demotools.IQuestioner,
 helper IScenarioHelper) MigrateUser {
 scenario := MigrateUser{
  helper:       helper,
  questioner:   questioner,
  resources:    Resources{},
  cognitoActor: &actions.CognitoActions{CognitoClient:
 cognitoidentityprovider.NewFromConfig(sdkConfig)},
 }
 scenario.resources.init(scenario.cognitoActor, questioner)
 return scenario
}

// AddMigrateUserTrigger adds a Lambda handler as an invocation target for the
 MigrateUser trigger.
func (runner *MigrateUser) AddMigrateUserTrigger(ctx context.Context, userPoolId
 string, functionArn string) {
 log.Printf("Let's add a Lambda function to handle the MigrateUser trigger from
 Cognito.\n" +
  "This trigger happens when an unknown user signs in, and lets your function
 take action before Cognito\n" +
```

```
  "rejects the user.\n\n")
 err := runner.cognitoActor.UpdateTriggers(
  ctx, userPoolId,
  actions.TriggerInfo{Trigger: actions.UserMigration, HandlerArn:
 aws.String(functionArn)})
 if err != nil {
  panic(err)
 }
 log.Printf("Lambda function %v added to user pool %v to handle the MigrateUser
 trigger.\n",
  functionArn, userPoolId)

 log.Println(strings.Repeat("-", 88))
}

// SignInUser adds a new user to the known users table and signs that user in to
 Amazon Cognito.
func (runner *MigrateUser) SignInUser(ctx context.Context, usersTable string,
 clientId string) (bool, actions.User) {
 log.Println("Let's sign in a user to your Cognito user pool. When the username
 and email matches an entry in the\n" +
  "DynamoDB known users table, the email is automatically verified and the user
 is migrated to the Cognito user pool.")

 user := actions.User{}
 user.UserName = runner.questioner.Ask("\nEnter a username:")
 user.UserEmail = runner.questioner.Ask("\nEnter an email that you own. This
 email will be used to confirm user migration\n" +
  "during this example:")

 runner.helper.AddKnownUser(ctx, usersTable, user)

 var err error
 var resetRequired *types.PasswordResetRequiredException
 var authResult *types.AuthenticationResultType
 signedIn := false
 for !signedIn && resetRequired == nil {
  log.Printf("Signing in to Cognito as user '%v'. The expected result is a
 PasswordResetRequiredException.\n\n", user.UserName)
  authResult, err = runner.cognitoActor.SignIn(ctx, clientId, user.UserName, "_")
  if err != nil {
   if errors.As(err, &resetRequired) {
    log.Printf("\nUser '%v' is not in the Cognito user pool but was found in the
 DynamoDB known users table.\n"+
```

```
     "User migration is started and a password reset is required.",
 user.UserName)
   } else {
    panic(err)
   }
  } else {
   log.Printf("User '%v' successfully signed in. This is unexpected and probably
 means you have not\n"+
    "cleaned up a previous run of this scenario, so the user exist in the Cognito
 user pool.\n"+
    "You can continue this example and select to clean up resources, or manually
 remove\n"+
    "the user from your user pool and try again.", user.UserName)
   runner.resources.userAccessTokens = append(runner.resources.userAccessTokens,
 *authResult.AccessToken)
   signedIn = true
  }
 }

 log.Println(strings.Repeat("-", 88))
 return resetRequired != nil, user
}

// ResetPassword starts a password recovery flow.
func (runner *MigrateUser) ResetPassword(ctx context.Context, clientId string,
 user actions.User) {
 wantCode := runner.questioner.AskBool(fmt.Sprintf("In order to migrate the user
 to Cognito, you must be able to receive a confirmation\n"+
  "code by email at %v. Do you want to send a code (y/n)?", user.UserEmail), "y")
 if !wantCode {
  log.Println("To complete this example and successfully migrate a user to
 Cognito, you must enter an email\n" +
   "you own that can receive a confirmation code.")
  return
 }
 codeDelivery, err := runner.cognitoActor.ForgotPassword(ctx, clientId,
 user.UserName)
 if err != nil {
  panic(err)
 }
 log.Printf("\nA confirmation code has been sent to %v.",
 *codeDelivery.Destination)
 code := runner.questioner.Ask("Check your email and enter it here:")
```

```
 confirmed := false
 password := runner.questioner.AskPassword("\nEnter a password that has at least
 eight characters, uppercase, lowercase, numbers and symbols.\n"+
  "(the password will not display as you type):", 8)
 for !confirmed {
  log.Printf("\nConfirming password reset for user '%v'.\n", user.UserName)
  err = runner.cognitoActor.ConfirmForgotPassword(ctx, clientId, code,
 user.UserName, password)
  if err != nil {
   var invalidPassword *types.InvalidPasswordException
   if errors.As(err, &invalidPassword) {
    password = runner.questioner.AskPassword("\nEnter another password:", 8)
   } else {
    panic(err)
   }
  } else {
   confirmed = true
  }
 }
 log.Printf("User '%v' successfully confirmed and migrated.\n", user.UserName)
 log.Println("Signing in with your username and password...")
 authResult, err := runner.cognitoActor.SignIn(ctx, clientId, user.UserName,
 password)
 if err != nil {
  panic(err)
 }
 log.Printf("Successfully signed in. Your access token starts with: %v...\n",
 (*authResult.AccessToken)[:10])
 runner.resources.userAccessTokens = append(runner.resources.userAccessTokens,
 *authResult.AccessToken)

 log.Println(strings.Repeat("-", 88))
}

// Run runs the scenario.
func (runner *MigrateUser) Run(ctx context.Context, stackName string) {
 defer func() {
  if r := recover(); r != nil {
   log.Println("Something went wrong with the demo.")
   runner.resources.Cleanup(ctx)
  }
 }()

 log.Println(strings.Repeat("-", 88))
```

```
 log.Printf("Welcome\n")

 log.Println(strings.Repeat("-", 88))

 stackOutputs, err := runner.helper.GetStackOutputs(ctx, stackName)
 if err != nil {
  panic(err)
 }
 runner.resources.userPoolId = stackOutputs["UserPoolId"]

 runner.AddMigrateUserTrigger(ctx, stackOutputs["UserPoolId"],
 stackOutputs["MigrateUserFunctionArn"])
 runner.resources.triggers = append(runner.resources.triggers,
 actions.UserMigration)
 resetNeeded, user := runner.SignInUser(ctx, stackOutputs["TableName"],
 stackOutputs["UserPoolClientId"])
 if resetNeeded {
  runner.helper.ListRecentLogEvents(ctx, stackOutputs["MigrateUserFunction"])
  runner.ResetPassword(ctx, stackOutputs["UserPoolClientId"], user)
 }

 runner.resources.Cleanup(ctx)

 log.Println(strings.Repeat("-", 88))
 log.Println("Thanks for watching!")
 log.Println(strings.Repeat("-", 88))
}
```

Gérez le déclencheur `MigrateUser` avec une fonction Lambda.

```
import (
 "context"
 "log"
 "os"

 "github.com/aws/aws-lambda-go/events"
 "github.com/aws/aws-lambda-go/lambda"
 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/config"
 "github.com/aws/aws-sdk-go-v2/feature/dynamodb/attributevalue"
```

```
 "github.com/aws/aws-sdk-go-v2/feature/dynamodb/expression"
 "github.com/aws/aws-sdk-go-v2/service/dynamodb"
)

const TABLE_NAME = "TABLE_NAME"

// UserInfo defines structured user data that can be marshalled to a DynamoDB
 format.
type UserInfo struct {
 UserName  string `dynamodbav:"UserName"`
 UserEmail string `dynamodbav:"UserEmail"`
}

type handler struct {
 dynamoClient *dynamodb.Client
}

// HandleRequest handles the MigrateUser event by looking up a user in an Amazon
 DynamoDB table and
// specifying whether they should be migrated to the user pool.
func (h *handler) HandleRequest(ctx context.Context, event
 events.CognitoEventUserPoolsMigrateUser)
 (events.CognitoEventUserPoolsMigrateUser, error) {
 log.Printf("Received migrate trigger from %v for user '%v'",
 event.TriggerSource, event.UserName)
 if event.TriggerSource != "UserMigration_Authentication" {
  return event, nil
 }
 tableName := os.Getenv(TABLE_NAME)
 user := UserInfo{
  UserName: event.UserName,
 }
 log.Printf("Looking up user '%v' in table %v.\n", user.UserName, tableName)
 filterEx := expression.Name("UserName").Equal(expression.Value(user.UserName))
 expr, err := expression.NewBuilder().WithFilter(filterEx).Build()
 if err != nil {
  log.Printf("Error building expression to query for user '%v'.\n",
 user.UserName)
  return event, err
 }
 output, err := h.dynamoClient.Scan(ctx, &dynamodb.ScanInput{
  TableName:                 aws.String(tableName),
  FilterExpression:          expr.Filter(),
  ExpressionAttributeNames:  expr.Names(),
```

```
  ExpressionAttributeValues: expr.Values(),
 })
 if err != nil {
  log.Printf("Error looking up user '%v'.\n", user.UserName)
  return event, err
 }
 if len(output.Items) == 0 {
  log.Printf("User '%v' not found, not migrating user.\n", user.UserName)
  return event, err
 }

 var users []UserInfo
 err = attributevalue.UnmarshalListOfMaps(output.Items, &users)
 if err != nil {
  log.Printf("Couldn't unmarshal DynamoDB items. Here's why: %v\n", err)
  return event, err
 }

 user = users[0]
 log.Printf("UserName '%v' found with email %v. User is migrated and must reset
 password.\n", user.UserName, user.UserEmail)
 event.CognitoEventUserPoolsMigrateUserResponse.UserAttributes =
 map[string]string{
  "email":          user.UserEmail,
  "email_verified": "true", // email_verified is required for the forgot password
 flow.
 }
 event.CognitoEventUserPoolsMigrateUserResponse.FinalUserStatus =
 "RESET_REQUIRED"
 event.CognitoEventUserPoolsMigrateUserResponse.MessageAction = "SUPPRESS"

 return event, err
}

func main() {
 ctx := context.Background()
 sdkConfig, err := config.LoadDefaultConfig(ctx)
 if err != nil {
  log.Panicln(err)
 }
 h := handler{
  dynamoClient: dynamodb.NewFromConfig(sdkConfig),
 }
 lambda.Start(h.HandleRequest)
```

```
}
```

Créez une structure qui exécute les tâches courantes.

```
import (
 "context"
 "log"
 "strings"
 "time"
 "user_pools_and_lambda_triggers/actions"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/service/cloudformation"
 "github.com/aws/aws-sdk-go-v2/service/cloudwatchlogs"
 "github.com/aws/aws-sdk-go-v2/service/dynamodb"
 "github.com/awsdocs/aws-doc-sdk-examples/gov2/demotools"
)

// IScenarioHelper defines common functions used by the workflows in this
 example.
type IScenarioHelper interface {
 Pause(secs int)
 GetStackOutputs(ctx context.Context, stackName string) (actions.StackOutputs,
 error)
 PopulateUserTable(ctx context.Context, tableName string)
 GetKnownUsers(ctx context.Context, tableName string) (actions.UserList, error)
 AddKnownUser(ctx context.Context, tableName string, user actions.User)
 ListRecentLogEvents(ctx context.Context, functionName string)
}

// ScenarioHelper contains AWS wrapper structs used by the workflows in this
 example.
type ScenarioHelper struct {
 questioner  demotools.IQuestioner
 dynamoActor *actions.DynamoActions
 cfnActor    *actions.CloudFormationActions
 cwlActor    *actions.CloudWatchLogsActions
 isTestRun   bool
}
```

```
// NewScenarioHelper constructs a new scenario helper.
func NewScenarioHelper(sdkConfig aws.Config, questioner demotools.IQuestioner)
 ScenarioHelper {
 scenario := ScenarioHelper{
  questioner:  questioner,
  dynamoActor: &actions.DynamoActions{DynamoClient:
 dynamodb.NewFromConfig(sdkConfig)},
  cfnActor:    &actions.CloudFormationActions{CfnClient:
 cloudformation.NewFromConfig(sdkConfig)},
  cwlActor:    &actions.CloudWatchLogsActions{CwlClient:
 cloudwatchlogs.NewFromConfig(sdkConfig)},
 }
 return scenario
}

// Pause waits for the specified number of seconds.
func (helper ScenarioHelper) Pause(secs int) {
 if !helper.isTestRun {
  time.Sleep(time.Duration(secs) * time.Second)
 }
}

// GetStackOutputs gets the outputs from the specified CloudFormation stack in a
 structured format.
func (helper ScenarioHelper) GetStackOutputs(ctx context.Context, stackName
 string) (actions.StackOutputs, error) {
 return helper.cfnActor.GetOutputs(ctx, stackName), nil
}

// PopulateUserTable fills the known user table with example data.
func (helper ScenarioHelper) PopulateUserTable(ctx context.Context, tableName
 string) {
 log.Printf("First, let's add some users to the DynamoDB %v table we'll use for
 this example.\n", tableName)
 err := helper.dynamoActor.PopulateTable(ctx, tableName)
 if err != nil {
  panic(err)
 }
}

// GetKnownUsers gets the users from the known users table in a structured
 format.
func (helper ScenarioHelper) GetKnownUsers(ctx context.Context, tableName string)
 (actions.UserList, error) {
```

```
 knownUsers, err := helper.dynamoActor.Scan(ctx, tableName)
 if err != nil {
  log.Printf("Couldn't get known users from table %v. Here's why: %v\n",
 tableName, err)
 }
 return knownUsers, err
}

// AddKnownUser adds a user to the known users table.
func (helper ScenarioHelper) AddKnownUser(ctx context.Context, tableName string,
 user actions.User) {
 log.Printf("Adding user '%v' with email '%v' to the DynamoDB known users
 table...\n",
  user.UserName, user.UserEmail)
 err := helper.dynamoActor.AddUser(ctx, tableName, user)
 if err != nil {
  panic(err)
 }
}

// ListRecentLogEvents gets the most recent log stream and events for the
 specified Lambda function and displays them.
func (helper ScenarioHelper) ListRecentLogEvents(ctx context.Context,
 functionName string) {
 log.Println("Waiting a few seconds to let Lambda write to CloudWatch Logs...")
 helper.Pause(10)
 log.Println("Okay, let's check the logs to find what's happened recently with
 your Lambda function.")
 logStream, err := helper.cwlActor.GetLatestLogStream(ctx, functionName)
 if err != nil {
  panic(err)
 }
 log.Printf("Getting some recent events from log stream %v\n",
 *logStream.LogStreamName)
 events, err := helper.cwlActor.GetLogEvents(ctx, functionName,
 *logStream.LogStreamName, 10)
 if err != nil {
  panic(err)
 }
 for _, event := range events {
  log.Printf("\t%v", *event.Message)
 }
 log.Println(strings.Repeat("-", 88))
}
```

Créez une structure qui encapsule les actions Amazon Cognito.

```
import (
 "context"
 "errors"
 "log"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/service/cognitoidentityprovider"
 "github.com/aws/aws-sdk-go-v2/service/cognitoidentityprovider/types"
)

type CognitoActions struct {
 CognitoClient *cognitoidentityprovider.Client
}



// Trigger and TriggerInfo define typed data for updating an Amazon Cognito
 trigger.
type Trigger int

const (
 PreSignUp Trigger = iota
 UserMigration
 PostAuthentication
)

type TriggerInfo struct {
 Trigger    Trigger
 HandlerArn *string
}

// UpdateTriggers adds or removes Lambda triggers for a user pool. When a trigger
 is specified with a `nil` value,
// it is removed from the user pool.
func (actor CognitoActions) UpdateTriggers(ctx context.Context, userPoolId
 string, triggers ...TriggerInfo) error {
```

```
 output, err := actor.CognitoClient.DescribeUserPool(ctx,
 &cognitoidentityprovider.DescribeUserPoolInput{
  UserPoolId: aws.String(userPoolId),
 })
 if err != nil {
  log.Printf("Couldn't get info about user pool %v. Here's why: %v\n",
 userPoolId, err)
  return err
 }
 lambdaConfig := output.UserPool.LambdaConfig
 for _, trigger := range triggers {
  switch trigger.Trigger {
  case PreSignUp:
   lambdaConfig.PreSignUp = trigger.HandlerArn
  case UserMigration:
   lambdaConfig.UserMigration = trigger.HandlerArn
  case PostAuthentication:
   lambdaConfig.PostAuthentication = trigger.HandlerArn
  }
 }
 _, err = actor.CognitoClient.UpdateUserPool(ctx,
 &cognitoidentityprovider.UpdateUserPoolInput{
  UserPoolId:   aws.String(userPoolId),
  LambdaConfig: lambdaConfig,
 })
 if err != nil {
  log.Printf("Couldn't update user pool %v. Here's why: %v\n", userPoolId, err)
 }
 return err
}



// SignUp signs up a user with Amazon Cognito.
func (actor CognitoActions) SignUp(ctx context.Context, clientId string, userName
 string, password string, userEmail string) (bool, error) {
 confirmed := false
 output, err := actor.CognitoClient.SignUp(ctx,
 &cognitoidentityprovider.SignUpInput{
  ClientId: aws.String(clientId),
  Password: aws.String(password),
  Username: aws.String(userName),
  UserAttributes: []types.AttributeType{
   {Name: aws.String("email"), Value: aws.String(userEmail)},
```

```
  },
 })
 if err != nil {
  var invalidPassword *types.InvalidPasswordException
  if errors.As(err, &invalidPassword) {
   log.Println(*invalidPassword.Message)
  } else {
   log.Printf("Couldn't sign up user %v. Here's why: %v\n", userName, err)
  }
 } else {
  confirmed = output.UserConfirmed
 }
 return confirmed, err
}



// SignIn signs in a user to Amazon Cognito using a username and password
 authentication flow.
func (actor CognitoActions) SignIn(ctx context.Context, clientId string, userName
 string, password string) (*types.AuthenticationResultType, error) {
 var authResult *types.AuthenticationResultType
 output, err := actor.CognitoClient.InitiateAuth(ctx,
 &cognitoidentityprovider.InitiateAuthInput{
  AuthFlow:       "USER_PASSWORD_AUTH",
  ClientId:       aws.String(clientId),
  AuthParameters: map[string]string{"USERNAME": userName, "PASSWORD": password},
 })
 if err != nil {
  var resetRequired *types.PasswordResetRequiredException
  if errors.As(err, &resetRequired) {
   log.Println(*resetRequired.Message)
  } else {
   log.Printf("Couldn't sign in user %v. Here's why: %v\n", userName, err)
  }
 } else {
  authResult = output.AuthenticationResult
 }
 return authResult, err
}
```

```
// ForgotPassword starts a password recovery flow for a user. This flow typically
 sends a confirmation code
// to the user's configured notification destination, such as email.
func (actor CognitoActions) ForgotPassword(ctx context.Context, clientId string,
 userName string) (*types.CodeDeliveryDetailsType, error) {
 output, err := actor.CognitoClient.ForgotPassword(ctx,
 &cognitoidentityprovider.ForgotPasswordInput{
  ClientId: aws.String(clientId),
  Username: aws.String(userName),
 })
 if err != nil {
  log.Printf("Couldn't start password reset for user '%v'. Here;s why: %v\n",
 userName, err)
 }
 return output.CodeDeliveryDetails, err
}



// ConfirmForgotPassword confirms a user with a confirmation code and a new
 password.
func (actor CognitoActions) ConfirmForgotPassword(ctx context.Context, clientId
 string, code string, userName string, password string) error {
 _, err := actor.CognitoClient.ConfirmForgotPassword(ctx,
 &cognitoidentityprovider.ConfirmForgotPasswordInput{
  ClientId:         aws.String(clientId),
  ConfirmationCode: aws.String(code),
  Password:         aws.String(password),
  Username:         aws.String(userName),
 })
 if err != nil {
  var invalidPassword *types.InvalidPasswordException
  if errors.As(err, &invalidPassword) {
   log.Println(*invalidPassword.Message)
  } else {
   log.Printf("Couldn't confirm user %v. Here's why: %v", userName, err)
  }
 }
 return err
}



// DeleteUser removes a user from the user pool.
```

```
func (actor CognitoActions) DeleteUser(ctx context.Context, userAccessToken
 string) error {
 _, err := actor.CognitoClient.DeleteUser(ctx,
 &cognitoidentityprovider.DeleteUserInput{
  AccessToken: aws.String(userAccessToken),
 })
 if err != nil {
  log.Printf("Couldn't delete user. Here's why: %v\n", err)
 }
 return err
}



// AdminCreateUser uses administrator credentials to add a user to a user pool.
 This method leaves the user
// in a state that requires they enter a new password next time they sign in.
func (actor CognitoActions) AdminCreateUser(ctx context.Context, userPoolId
 string, userName string, userEmail string) error {
 _, err := actor.CognitoClient.AdminCreateUser(ctx,
 &cognitoidentityprovider.AdminCreateUserInput{
  UserPoolId:     aws.String(userPoolId),
  Username:       aws.String(userName),
  MessageAction:  types.MessageActionTypeSuppress,
  UserAttributes: []types.AttributeType{{Name: aws.String("email"), Value:
 aws.String(userEmail)}},
 })
 if err != nil {
  var userExists *types.UsernameExistsException
  if errors.As(err, &userExists) {
   log.Printf("User %v already exists in the user pool.", userName)
   err = nil
  } else {
   log.Printf("Couldn't create user %v. Here's why: %v\n", userName, err)
  }
 }
 return err
}



// AdminSetUserPassword uses administrator credentials to set a password for a
 user without requiring a
// temporary password.
```

```
func (actor CognitoActions) AdminSetUserPassword(ctx context.Context, userPoolId
 string, userName string, password string) error {
 _, err := actor.CognitoClient.AdminSetUserPassword(ctx,
 &cognitoidentityprovider.AdminSetUserPasswordInput{
  Password:   aws.String(password),
  UserPoolId: aws.String(userPoolId),
  Username:   aws.String(userName),
  Permanent:  true,
 })
 if err != nil {
  var invalidPassword *types.InvalidPasswordException
  if errors.As(err, &invalidPassword) {
   log.Println(*invalidPassword.Message)
  } else {
   log.Printf("Couldn't set password for user %v. Here's why: %v\n", userName,
 err)
  }
 }
 return err
}
```

Créez une structure qui encapsule les actions DynamoDB.

```
import (
 "context"
 "fmt"
 "log"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/feature/dynamodb/attributevalue"
 "github.com/aws/aws-sdk-go-v2/service/dynamodb"
 "github.com/aws/aws-sdk-go-v2/service/dynamodb/types"
)

// DynamoActions encapsulates the Amazon Simple Notification Service (Amazon SNS)
 actions
// used in the examples.
type DynamoActions struct {
 DynamoClient *dynamodb.Client
}
```

```
// User defines structured user data.
type User struct {
 UserName  string
 UserEmail string
 LastLogin *LoginInfo `dynamodbav:",omitempty"`
}

// LoginInfo defines structured custom login data.
type LoginInfo struct {
 UserPoolId string
 ClientId   string
 Time       string
}

// UserList defines a list of users.
type UserList struct {
 Users []User
}

// UserNameList returns the usernames contained in a UserList as a list of
 strings.
func (users *UserList) UserNameList() []string {
 names := make([]string, len(users.Users))
 for i := 0; i < len(users.Users); i++ {
  names[i] = users.Users[i].UserName
 }
 return names
}

// PopulateTable adds a set of test users to the table.
func (actor DynamoActions) PopulateTable(ctx context.Context, tableName string)
 error {
 var err error
 var item map[string]types.AttributeValue
 var writeReqs []types.WriteRequest
 for i := 1; i < 4; i++ {
  item, err = attributevalue.MarshalMap(User{UserName: fmt.Sprintf("test_user_
%v", i), UserEmail: fmt.Sprintf("test_email_%v@example.com", i)})
  if err != nil {
   log.Printf("Couldn't marshall user into DynamoDB format. Here's why: %v\n",
 err)
   return err
  }
```

```
  writeReqs = append(writeReqs, types.WriteRequest{PutRequest:
 &types.PutRequest{Item: item}})
 }
 _, err = actor.DynamoClient.BatchWriteItem(ctx, &dynamodb.BatchWriteItemInput{
  RequestItems: map[string][]types.WriteRequest{tableName: writeReqs},
 })
 if err != nil {
  log.Printf("Couldn't populate table %v with users. Here's why: %v\n",
 tableName, err)
 }
 return err
}

// Scan scans the table for all items.
func (actor DynamoActions) Scan(ctx context.Context, tableName string) (UserList,
 error) {
 var userList UserList
 output, err := actor.DynamoClient.Scan(ctx, &dynamodb.ScanInput{
  TableName: aws.String(tableName),
 })
 if err != nil {
  log.Printf("Couldn't scan table %v for items. Here's why: %v\n", tableName,
 err)
 } else {
  err = attributevalue.UnmarshalListOfMaps(output.Items, &userList.Users)
  if err != nil {
   log.Printf("Couldn't unmarshal items into users. Here's why: %v\n", err)
  }
 }
 return userList, err
}

// AddUser adds a user item to a table.
func (actor DynamoActions) AddUser(ctx context.Context, tableName string, user
 User) error {
 userItem, err := attributevalue.MarshalMap(user)
 if err != nil {
  log.Printf("Couldn't marshall user to item. Here's why: %v\n", err)
 }
 _, err = actor.DynamoClient.PutItem(ctx, &dynamodb.PutItemInput{
  Item:      userItem,
  TableName: aws.String(tableName),
 })
 if err != nil {
```

```
  log.Printf("Couldn't put item in table %v. Here's why: %v", tableName, err)
 }
 return err
}
```

Créez une structure qui enveloppe CloudWatch Enregistre les actions.

```
import (
 "context"
 "fmt"
 "log"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/service/cloudwatchlogs"
 "github.com/aws/aws-sdk-go-v2/service/cloudwatchlogs/types"
)

type CloudWatchLogsActions struct {
 CwlClient *cloudwatchlogs.Client
}

// GetLatestLogStream gets the most recent log stream for a Lambda function.
func (actor CloudWatchLogsActions) GetLatestLogStream(ctx context.Context,
 functionName string) (types.LogStream, error) {
 var logStream types.LogStream
 logGroupName := fmt.Sprintf("/aws/lambda/%s", functionName)
 output, err := actor.CwlClient.DescribeLogStreams(ctx,
 &cloudwatchlogs.DescribeLogStreamsInput{
  Descending:   aws.Bool(true),
  Limit:        aws.Int32(1),
  LogGroupName: aws.String(logGroupName),
  OrderBy:      types.OrderByLastEventTime,
 })
 if err != nil {
  log.Printf("Couldn't get log streams for log group %v. Here's why: %v\n",
 logGroupName, err)
 } else {
  logStream = output.LogStreams[0]
 }
 return logStream, err
```

```
}

// GetLogEvents gets the most recent eventCount events from the specified log
 stream.
func (actor CloudWatchLogsActions) GetLogEvents(ctx context.Context, functionName
 string, logStreamName string, eventCount int32) (
 []types.OutputLogEvent, error) {
 var events []types.OutputLogEvent
 logGroupName := fmt.Sprintf("/aws/lambda/%s", functionName)
 output, err := actor.CwlClient.GetLogEvents(ctx,
 &cloudwatchlogs.GetLogEventsInput{
  LogStreamName: aws.String(logStreamName),
  Limit:         aws.Int32(eventCount),
  LogGroupName:  aws.String(logGroupName),
 })
 if err != nil {
  log.Printf("Couldn't get log event for log stream %v. Here's why: %v\n",
 logStreamName, err)
 } else {
  events = output.Events
 }
 return events, err
}
```

Créez une structure qui enveloppe CloudFormation actions.

```
import (
 "context"
 "log"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/service/cloudformation"
)

// StackOutputs defines a map of outputs from a specific stack.
type StackOutputs map[string]string

type CloudFormationActions struct {
 CfnClient *cloudformation.Client
}
```

```
// GetOutputs gets the outputs from a CloudFormation stack and puts them into a
 structured format.
func (actor CloudFormationActions) GetOutputs(ctx context.Context, stackName
 string) StackOutputs {
 output, err := actor.CfnClient.DescribeStacks(ctx,
 &cloudformation.DescribeStacksInput{
  StackName: aws.String(stackName),
 })
 if err != nil || len(output.Stacks) == 0 {
  log.Panicf("Couldn't find a CloudFormation stack named %v. Here's why: %v\n",
 stackName, err)
 }
 stackOutputs := StackOutputs{}
 for _, out := range output.Stacks[0].Outputs {
  stackOutputs[*out.OutputKey] = *out.OutputValue
 }
 return stackOutputs
}
```

Nettoyez les ressources.

```
import (
 "context"
 "log"
 "user_pools_and_lambda_triggers/actions"

 "github.com/awsdocs/aws-doc-sdk-examples/gov2/demotools"
)

// Resources keeps track of AWS resources created during an example and handles
// cleanup when the example finishes.
type Resources struct {
 userPoolId       string
 userAccessTokens []string
 triggers         []actions.Trigger

 cognitoActor *actions.CognitoActions
 questioner   demotools.IQuestioner
}
```

```
func (resources *Resources) init(cognitoActor *actions.CognitoActions, questioner
 demotools.IQuestioner) {
 resources.userAccessTokens = []string{}
 resources.triggers = []actions.Trigger{}
 resources.cognitoActor = cognitoActor
 resources.questioner = questioner
}

// Cleanup deletes all AWS resources created during an example.
func (resources *Resources) Cleanup(ctx context.Context) {
 defer func() {
  if r := recover(); r != nil {
   log.Printf("Something went wrong during cleanup.\n%v\n", r)
   log.Println("Use the AWS Management Console to remove any remaining resources
 \n" +
    "that were created for this scenario.")
  }
 }()

 wantDelete := resources.questioner.AskBool("Do you want to remove all of the AWS
 resources that were created "+
  "during this demo (y/n)?", "y")
 if wantDelete {
  for _, accessToken := range resources.userAccessTokens {
   err := resources.cognitoActor.DeleteUser(ctx, accessToken)
   if err != nil {
    log.Println("Couldn't delete user during cleanup.")
    panic(err)
   }
   log.Println("Deleted user.")
  }
  triggerList := make([]actions.TriggerInfo, len(resources.triggers))
  for i := 0; i < len(resources.triggers); i++ {
   triggerList[i] = actions.TriggerInfo{Trigger: resources.triggers[i],
 HandlerArn: nil}
  }
  err := resources.cognitoActor.UpdateTriggers(ctx, resources.userPoolId,
 triggerList...)
  if err != nil {
   log.Println("Couldn't update Cognito triggers during cleanup.")
   panic(err)
  }
  log.Println("Removed Cognito triggers from user pool.")
```

```
 } else {
  log.Println("Be sure to remove resources when you're done with them to avoid
 unexpected charges!")
 }
}
```

- Pour plus de détails sur l'API, consultez les rubriques suivantes dans la Référence des API du kit AWS SDK pour Go .
  - ConfirmForgotPassword
  - DeleteUser
  - ForgotPassword
  - InitiateAuth
  - SignUp
  - UpdateUserPool

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Créez une API REST API Gateway pour effectuer le suivi COVID-19 données

L'exemple de code suivant montre comment créer une API REST qui simule un système pour suivre les cas quotidiens de COVID-19 aux États-Unis, à l'aide de données fictives.

Python

Kit SDK for Python (Boto3)

Montre comment utiliser AWS Calice avec AWS SDK pour Python (Boto3) pour créer une API REST sans serveur qui utilise Amazon API Gateway, AWS Lambda et Amazon DynamoDB. L'API REST simule un système qui suit les cas quotidiens de COVID-19 aux États-Unis, à l'aide de données fictives. Découvrez comment :

- Utiliser AWS Chalice pour définir des itinéraires dans les fonctions Lambda qui sont appelées pour gérer les requêtes REST provenant d'API Gateway.

- Utilisez les fonctions Lambda pour récupérer et stocker des données dans une table DynamoDB afin de répondre aux demandes REST.
- Définissez la structure des tables et les ressources relatives aux rôles de sécurité dans un AWS CloudFormation modèle.
- Utiliser AWS Calice et CloudFormation pour regrouper et déployer toutes les ressources nécessaires.
- Utiliser CloudFormation pour nettoyer toutes les ressources créées.

Pour le code source complet et les instructions de configuration et d'exécution, consultez l'exemple complet sur GitHub.

Les services utilisés dans cet exemple

- API Gateway
- CloudFormation
- DynamoDB
- Lambda

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Créer une API REST de bibliothèque de prêt

L'exemple de code suivant montre comment créer une bibliothèque de prêt dans laquelle les clients peuvent emprunter et retourner des livres à l'aide d'une API REST soutenue par une base de données Amazon Aurora.

Python

Kit SDK for Python (Boto3)

Montre comment utiliser AWS SDK pour Python (Boto3) avec l'API Amazon Relational Database Service (Amazon RDS) et AWS Chalice pour créer une API REST soutenue par une base de données Amazon Aurora. Le service Web est entièrement sans serveur et représente une bibliothèque de prêt simple où les clients peuvent emprunter et retourner des livres. Découvrez comment :

- Créer et gérer un cluster de bases de données Aurora sans serveur.
- Utiliser AWS Secrets Manager pour gérer les informations d'identification de base de données.
- Implémenter une couche de stockage de données qui utilise Amazon RDS pour déplacer des données vers et hors de la base de données.
- Utiliser AWS Chalice va déployer une API REST sans serveur sur Amazon API Gateway et AWS Lambda.
- Utiliser le package Requests (Requêtes) pour envoyer des requêtes au service web.

Pour le code source complet et les instructions de configuration et d'exécution, consultez l'exemple complet sur GitHub.

Les services utilisés dans cet exemple

- API Gateway
- Aurora
- Lambda
- Secrets Manager

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Créer une application de messagerie avec Step Functions

L'exemple de code suivant montre comment créer un AWS Step Functions application de messagerie qui récupère les enregistrements de messages à partir d'une table de base de données.

Python

Kit SDK for Python (Boto3)

Montre comment utiliser AWS SDK pour Python (Boto3) avec AWS Step Functions pour créer une application de messagerie qui extrait les enregistrements de messages d'une table Amazon DynamoDB et les envoie via Amazon Simple Queue Service (Amazon SQS). La machine à états s'intègre à un AWS Lambda fonction pour scanner la base de données à la recherche de messages non envoyés.

- Créez une machine d'état qui extrait et met à jour des enregistrements de message d'une table Amazon DynamoDB.
- Mettez à jour la définition de la machine d'état pour envoyer des messages à Amazon Simple Queue Service (Amazon SQS).
- Démarrez et arrêtez les exécutions de la machine.
- Connectez-vous à Lambda, DynamoDB et Amazon SQS à partir d'une machine d'état à l'aide d'intégrations de services.

Pour le code source complet et les instructions de configuration et d'exécution, consultez l'exemple complet sur GitHub.

Les services utilisés dans cet exemple

- DynamoDB
- Lambda
- Amazon SQS
- Fonctions de l'étape

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Création d'une API REST avec intégration de fonctions proxy

L'exemple de code suivant illustre comment :

- Création d'un rôle IAM pour l'exécution de Lambda
- Création et déploiement d'une fonction Lambda
- Création d'une API REST
- Configurer l'intégration du proxy Lambda
- Déploiement et test de l'API
- nettoyer des ressources ;

Bash

AWS CLI avec le script Bash

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code.

```
#!/bin/bash

set -euo pipefail

# Simple API Gateway Lambda Integration Script
# This script creates a REST API with Lambda proxy integration

# Generate random identifiers
FUNCTION_NAME="GetStartedLambdaProxyIntegration-$(openssl rand -hex 4)"
ROLE_NAME="GetStartedLambdaBasicExecutionRole-$(openssl rand -hex 4)"
API_NAME="LambdaProxyAPI-$(openssl rand -hex 4)"

# Get AWS account info
ACCOUNT_ID=$(aws sts get-caller-identity --query Account --output text)
REGION=$(aws configure get region || echo "us-east-1")

# Validate inputs
if [[ -z "$ACCOUNT_ID" ]] || [[ -z "$REGION" ]]; then
    echo "Error: Failed to retrieve AWS account information" >&2
    exit 1
fi

echo "Creating Lambda function code..."

# Create Lambda function code with input validation
cat > lambda_function.py << 'EOF'
import json
import logging

logger = logging.getLogger()
logger.setLevel(logging.INFO)
```

```
def lambda_handler(event, context):
    try:
        logger.info("Received event: %s", json.dumps(event))

        greeter = 'World'

        # Safely retrieve greeter from query string parameters
        query_params = event.get('queryStringParameters') or {}
        if isinstance(query_params, dict) and 'greeter' in query_params:
            greeter_value = query_params.get('greeter')
            if isinstance(greeter_value, str) and greeter_value:
                greeter = greeter_value

        # Safely retrieve greeter from multi-value headers
        multi_headers = event.get('multiValueHeaders') or {}
        if isinstance(multi_headers, dict) and 'greeter' in multi_headers:
            greeter_list = multi_headers.get('greeter', [])
            if isinstance(greeter_list, list) and greeter_list:
                greeter = " and ".join(str(g) for g in greeter_list if g)

        # Safely retrieve greeter from headers
        headers = event.get('headers') or {}
        if isinstance(headers, dict) and 'greeter' in headers:
            greeter_value = headers.get('greeter')
            if isinstance(greeter_value, str) and greeter_value:
                greeter = greeter_value

        # Safely retrieve greeter from body
        body = event.get('body')
        if body and isinstance(body, str):
            try:
                body_dict = json.loads(body)
                if isinstance(body_dict, dict) and 'greeter' in body_dict:
                    greeter_value = body_dict.get('greeter')
                    if isinstance(greeter_value, str) and greeter_value:
                        greeter = greeter_value
            except (json.JSONDecodeError, ValueError) as e:
                logger.warning("Failed to parse body: %s", str(e))

        # Sanitize greeter to prevent injection
        greeter = greeter.replace('"', '\\"').replace("'", "\\'")

        response = {
            "statusCode": 200,
```

```
            "headers": {
                "Content-Type": "application/json"
            },
            "body": json.dumps({"message": f"Hello, {greeter}!"})
        }

        logger.info("Response: %s", json.dumps(response))
        return response

    except Exception as e:
        logger.error("Unexpected error: %s", str(e), exc_info=True)
        return {
            "statusCode": 500,
            "headers": {
                "Content-Type": "application/json"
            },
            "body": json.dumps({"error": "Internal server error"})
        }
EOF

# Create deployment package
zip -q function.zip lambda_function.py || {
    echo "Error: Failed to create function.zip" >&2
    exit 1
}

echo "Creating IAM role..."

# Create IAM trust policy
cat > trust-policy.json << 'EOF'
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
EOF
```

```
# Create IAM role with error handling
aws iam create-role \
    --role-name "$ROLE_NAME" \
    --assume-role-policy-document file://trust-policy.json \
    --description "Temporary role for Lambda execution" || {
    echo "Error: Failed to create IAM role" >&2
    exit 1
}

aws iam tag-role --role-name "$ROLE_NAME" --tags Key=project,Value=doc-smith
 Key=tutorial,Value=apigateway-lambda-integration

# Attach execution policy
aws iam attach-role-policy \
    --role-name "$ROLE_NAME" \
    --policy-arn "arn:aws:iam::aws:policy/service-role/
AWSLambdaBasicExecutionRole" || {
    echo "Error: Failed to attach IAM policy" >&2
    exit 1
}

# Wait for role propagation
sleep 15

echo "Creating Lambda function..."

# Create Lambda function with Python 3.11 (more recent runtime)
aws lambda create-function \
    --function-name "$FUNCTION_NAME" \
    --runtime python3.11 \
    --role "arn:aws:iam::$ACCOUNT_ID:role/$ROLE_NAME" \
    --handler lambda_function.lambda_handler \
    --zip-file fileb://function.zip \
    --timeout 30 \
    --memory-size 128 \
    --environment "Variables={LOG_LEVEL=INFO}" \
    --tags project=doc-smith,tutorial=apigateway-lambda-integration || {
    echo "Error: Failed to create Lambda function" >&2
    exit 1
}

echo "Creating API Gateway..."

# Create REST API with minimum logging
```

```
API_RESPONSE=$(aws apigateway create-rest-api \
    --name "$API_NAME" \
    --endpoint-configuration types=REGIONAL \
    --description "API for Lambda proxy integration tutorial" \
    --tags project=doc-smith,tutorial=apigateway-lambda-integration \
    --output json)

API_ID=$(echo "$API_RESPONSE" | grep -o '"id": "[^"]*"' | head -1 | cut -d'"' -
f4)

if [[ -z "$API_ID" ]]; then
    echo "Error: Failed to create API Gateway" >&2
    exit 1
fi

# Get root resource ID
ROOT_RESOURCE_ID=$(aws apigateway get-resources --rest-api-id "$API_ID" --query
 'items[?path==`/`].id' --output text)

# Create helloworld resource
aws apigateway create-resource \
    --rest-api-id "$API_ID" \
    --parent-id "$ROOT_RESOURCE_ID" \
    --path-part helloworld || {
    echo "Error: Failed to create resource" >&2
    exit 1
}

# Get resource ID
RESOURCE_ID=$(aws apigateway get-resources --rest-api-id "$API_ID" --query
 "items[?pathPart=='helloworld'].id" --output text)

# Create ANY method with no authorization (intentional for tutorial)
aws apigateway put-method \
    --rest-api-id "$API_ID" \
    --resource-id "$RESOURCE_ID" \
    --http-method ANY \
    --authorization-type NONE || {
    echo "Error: Failed to create method" >&2
    exit 1
}

# Set up Lambda proxy integration
```

```
LAMBDA_URI="arn:aws:apigateway:$REGION:lambda:path/2015-03-31/functions/
arn:aws:lambda:$REGION:$ACCOUNT_ID:function:$FUNCTION_NAME/invocations"

aws apigateway put-integration \
    --rest-api-id "$API_ID" \
    --resource-id "$RESOURCE_ID" \
    --http-method ANY \
    --type AWS_PROXY \
    --integration-http-method POST \
    --uri "$LAMBDA_URI" || {
    echo "Error: Failed to create integration" >&2
    exit 1
}

# Grant API Gateway permission to invoke Lambda
STATEMENT_ID="apigateway-invoke-$(openssl rand -hex 4)"
SOURCE_ARN="arn:aws:execute-api:$REGION:$ACCOUNT_ID:$API_ID/*/*"

aws lambda add-permission \
    --function-name "$FUNCTION_NAME" \
    --statement-id "$STATEMENT_ID" \
    --action lambda:InvokeFunction \
    --principal apigateway.amazonaws.com \
    --source-arn "$SOURCE_ARN" || {
    echo "Error: Failed to add Lambda permission" >&2
    exit 1
}

# Deploy API
aws apigateway create-deployment \
    --rest-api-id "$API_ID" \
    --stage-name test \
    --description "Test deployment" || {
    echo "Error: Failed to deploy API" >&2
    exit 1
}

echo "Testing API..."

# Test the API
INVOKE_URL="https://$API_ID.execute-api.$REGION.amazonaws.com/test/helloworld"

echo "API URL: $INVOKE_URL"
```

```
# Test with query parameter (with proper URL encoding)
echo "Testing with query parameter:"
curl -s -X GET "$INVOKE_URL?greeter=John" | jq . 2>/dev/null || curl -s -X GET
 "$INVOKE_URL?greeter=John"
echo ""

# Test with header
echo "Testing with header:"
curl -s -X GET "$INVOKE_URL" \
    -H 'content-type: application/json' \
    -H 'greeter: John' | jq . 2>/dev/null || curl -s -X GET "$INVOKE_URL" \
    -H 'content-type: application/json' \
    -H 'greeter: John'
echo ""

# Test with body
echo "Testing with POST body:"
curl -s -X POST "$INVOKE_URL" \
    -H 'content-type: application/json' \
    -d '{"greeter": "John"}' | jq . 2>/dev/null || curl -s -X POST "$INVOKE_URL"
 \
    -H 'content-type: application/json' \
    -d '{"greeter": "John"}'
echo ""

echo "Tutorial completed! API is available at: $INVOKE_URL"

# Cleanup
echo "Cleaning up resources..."

# Delete API
aws apigateway delete-rest-api --rest-api-id "$API_ID" || echo "Warning: Failed
 to delete API" >&2

# Delete Lambda function
aws lambda delete-function --function-name "$FUNCTION_NAME" || echo "Warning:
 Failed to delete Lambda function" >&2

# Detach policy and delete role
aws iam detach-role-policy \
    --role-name "$ROLE_NAME" \
    --policy-arn "arn:aws:iam::aws:policy/service-role/
AWSLambdaBasicExecutionRole" || echo "Warning: Failed to detach policy" >&2
```

```
aws iam delete-role --role-name "$ROLE_NAME" || echo "Warning: Failed to delete
 role" >&2

# Clean up local files securely
rm -f lambda_function.py function.zip trust-policy.json

echo "Cleanup completed!"
```

- Pour plus de détails sur l'API, consultez les rubriques suivantes dans la Référence des commandes de l'AWS CLI .
  - AddPermission
  - AttachRolePolicy
  - CreateDeployment
  - CreateFunction
  - CreateResource
  - CreateRestApi
  - CreateRole
  - DeleteFunction
  - DeleteRestApi
  - DeleteRole
  - DetachRolePolicy
  - GetCallerIdentity
  - GetResources
  - GetRestApis
  - PutIntegration
  - PutMethod

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Création d'une application de gestion des ressources photographiques permettant aux utilisateurs de gérer les photos à l'aide d'étiquettes

Les exemples de code suivants montrent comment créer une application sans serveur permettant aux utilisateurs de gérer des photos à l'aide d'étiquettes.

.NET

SDK pour .NET

Montre comment développer une application de gestion de ressources photographiques qui détecte les étiquettes dans les images à l'aide d'Amazon Rekognition et les stocke pour les récupérer ultérieurement.

Pour le code source complet et les instructions de configuration et d'exécution, consultez l'exemple complet sur GitHub.

Pour explorer en profondeur l'origine de cet exemple, consultez l'article sur AWS Community.

Les services utilisés dans cet exemple

- API Gateway
- DynamoDB
- Lambda
- Amazon Rekognition
- Amazon S3
- Amazon SNS

C++

SDK pour C++

Montre comment développer une application de gestion de ressources photographiques qui détecte les étiquettes dans les images à l'aide d'Amazon Rekognition et les stocke pour les récupérer ultérieurement.

Pour le code source complet et les instructions de configuration et d'exécution, consultez l'exemple complet sur GitHub.

Pour explorer en profondeur l'origine de cet exemple, consultez l'article sur AWS Community.

Les services utilisés dans cet exemple

- API Gateway
- DynamoDB
- Lambda
- Amazon Rekognition
- Amazon S3
- Amazon SNS

Java

SDK pour Java 2.x

Montre comment développer une application de gestion de ressources photographiques qui détecte les étiquettes dans les images à l'aide d'Amazon Rekognition et les stocke pour les récupérer ultérieurement.

Pour le code source complet et les instructions de configuration et d'exécution, consultez l'exemple complet sur GitHub.

Pour explorer en profondeur l'origine de cet exemple, consultez l'article sur AWS Community.

Les services utilisés dans cet exemple

- API Gateway
- DynamoDB
- Lambda
- Amazon Rekognition
- Amazon S3
- Amazon SNS

JavaScript

SDK pour JavaScript (v3)

Montre comment développer une application de gestion de ressources photographiques qui détecte les étiquettes dans les images à l'aide d'Amazon Rekognition et les stocke pour les récupérer ultérieurement.

Pour le code source complet et les instructions de configuration et d'exécution, consultez l'exemple complet sur GitHub.

Pour explorer en profondeur l'origine de cet exemple, consultez l'article sur AWS Community.

Les services utilisés dans cet exemple

- API Gateway
- DynamoDB
- Lambda
- Amazon Rekognition
- Amazon S3
- Amazon SNS

Kotlin

SDK pour Kotlin

Montre comment développer une application de gestion de ressources photographiques qui détecte les étiquettes dans les images à l'aide d'Amazon Rekognition et les stocke pour les récupérer ultérieurement.

Pour le code source complet et les instructions de configuration et d'exécution, consultez l'exemple complet sur GitHub.

Pour explorer en profondeur l'origine de cet exemple, consultez l'article sur AWS Community.

Les services utilisés dans cet exemple

- API Gateway
- DynamoDB
- Lambda
- Amazon Rekognition
- Amazon S3
- Amazon SNS

PHP

Kit SDK pour PHP

Montre comment développer une application de gestion de ressources photographiques qui détecte les étiquettes dans les images à l'aide d'Amazon Rekognition et les stocke pour les récupérer ultérieurement.

Pour le code source complet et les instructions de configuration et d'exécution, consultez l'exemple complet sur GitHub.

Pour explorer en profondeur l'origine de cet exemple, consultez l'article sur AWS Community.

Les services utilisés dans cet exemple

- API Gateway
- DynamoDB
- Lambda
- Amazon Rekognition
- Amazon S3
- Amazon SNS

Rust

SDK pour Rust

Montre comment développer une application de gestion de ressources photographiques qui détecte les étiquettes dans les images à l'aide d'Amazon Rekognition et les stocke pour les récupérer ultérieurement.

Pour le code source complet et les instructions de configuration et d'exécution, consultez l'exemple complet sur GitHub.

Pour explorer en profondeur l'origine de cet exemple, consultez l'article sur AWS Community.

Les services utilisés dans cet exemple

- API Gateway
- DynamoDB
- Lambda

- Amazon Rekognition
- Amazon S3
- Amazon SNS

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Créer une application de chat Websocket avec API Gateway

L'exemple de code suivant montre comment créer une application de chat desservie par une API Websocket basée sur Amazon API Gateway.

Python

Kit SDK for Python (Boto3)

Montre comment utiliser AWS SDK pour Python (Boto3) avec Amazon API Gateway V2 pour créer une API Websocket qui s'intègre à AWS Lambda et Amazon DynamoDB.

- Créez une API WebSocket dans API Gateway.
- Définissez un gestionnaire Lambda qui stocke les connexions dans DynamoDB et publie des messages pour d'autres participants au chat.
- Connectez-vous à l'application de chat Websocket et envoyez des messages avec le package Websockets.

Pour le code source complet et les instructions de configuration et d'exécution, consultez l'exemple complet sur GitHub.

Les services utilisés dans cet exemple

- API Gateway
- DynamoDB
- Lambda

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Créez une application qui analyse les commentaires des clients et synthétise le son

Les exemples de code suivants montrent comment créer une application qui analyse les cartes de commentaires des clients, les traduit depuis leur langue d'origine, détermine leur sentiment et génère un fichier audio à partir du texte traduit.

.NET

SDK pour .NET

Cet exemple d'application analyse et stocke les cartes de commentaires des clients. Plus précisément, elle répond aux besoins d'un hôtel fictif situé à New York. L'hôtel reçoit les commentaires des clients dans différentes langues sous la forme de cartes de commentaires physiques. Ces commentaires sont chargés dans l'application via un client Web. Après avoir chargé l'image d'une carte de commentaires, les étapes suivantes se déroulent :

- Le texte est extrait de l'image à l'aide d'Amazon Textract.
- Amazon Comprehend détermine le sentiment du texte extrait et sa langue.
- Le texte extrait est traduit en anglais à l'aide d'Amazon Translate.
- Amazon Polly synthétise un fichier audio à partir du texte extrait.

L'application complète peut être déployée avec AWS CDK. Pour le code source et les instructions de déploiement, consultez le projet dans GitHub.

Les services utilisés dans cet exemple

- Amazon Comprehend
- Lambda
- Amazon Polly
- Amazon Textract
- Amazon Translate

Java

SDK pour Java 2.x

Cet exemple d'application analyse et stocke les cartes de commentaires des clients. Plus précisément, elle répond aux besoins d'un hôtel fictif situé à New York. L'hôtel reçoit les

commentaires des clients dans différentes langues sous la forme de cartes de commentaires physiques. Ces commentaires sont chargés dans l'application via un client Web. Après avoir chargé l'image d'une carte de commentaires, les étapes suivantes se déroulent :

- Le texte est extrait de l'image à l'aide d'Amazon Textract.
- Amazon Comprehend détermine le sentiment du texte extrait et sa langue.
- Le texte extrait est traduit en anglais à l'aide d'Amazon Translate.
- Amazon Polly synthétise un fichier audio à partir du texte extrait.

L'application complète peut être déployée avec AWS CDK. Pour le code source et les instructions de déploiement, consultez le projet dans GitHub.

Les services utilisés dans cet exemple

- Amazon Comprehend
- Lambda
- Amazon Polly
- Amazon Textract
- Amazon Translate

JavaScript

SDK pour JavaScript (v3)

Cet exemple d'application analyse et stocke les cartes de commentaires des clients. Plus précisément, elle répond aux besoins d'un hôtel fictif situé à New York. L'hôtel reçoit les commentaires des clients dans différentes langues sous la forme de cartes de commentaires physiques. Ces commentaires sont chargés dans l'application via un client Web. Après avoir chargé l'image d'une carte de commentaires, les étapes suivantes se déroulent :

- Le texte est extrait de l'image à l'aide d'Amazon Textract.
- Amazon Comprehend détermine le sentiment du texte extrait et sa langue.
- Le texte extrait est traduit en anglais à l'aide d'Amazon Translate.
- Amazon Polly synthétise un fichier audio à partir du texte extrait.

L'application complète peut être déployée avec AWS CDK. Pour le code source et les instructions de déploiement, consultez le projet dans GitHub. Les extraits suivants montrent comment AWS SDK pour JavaScript est utilisé dans les fonctions Lambda.

```
import {
  ComprehendClient,
  DetectDominantLanguageCommand,
  DetectSentimentCommand,
} from "@aws-sdk/client-comprehend";

/**
 * Determine the language and sentiment of the extracted text.
 *
 * @param {{ source_text: string}} extractTextOutput
 */
export const handler = async (extractTextOutput) => {
  const comprehendClient = new ComprehendClient({});

  const detectDominantLanguageCommand = new DetectDominantLanguageCommand({
    Text: extractTextOutput.source_text,
  });

  // The source language is required for sentiment analysis and
  // translation in the next step.
  const { Languages } = await comprehendClient.send(
    detectDominantLanguageCommand,
  );

  const languageCode = Languages[0].LanguageCode;

  const detectSentimentCommand = new DetectSentimentCommand({
    Text: extractTextOutput.source_text,
    LanguageCode: languageCode,
  });

  const { Sentiment } = await comprehendClient.send(detectSentimentCommand);

  return {
    sentiment: Sentiment,
    language_code: languageCode,
  };
};
```

```
import {
  DetectDocumentTextCommand,
  TextractClient,
} from "@aws-sdk/client-textract";
```

```
/**
 * Fetch the S3 object from the event and analyze it using Amazon Textract.
 *
 * @param {import("@types/aws-lambda").EventBridgeEvent<"Object Created">}
 eventBridgeS3Event
 */
export const handler = async (eventBridgeS3Event) => {
  const textractClient = new TextractClient();

  const detectDocumentTextCommand = new DetectDocumentTextCommand({
    Document: {
      S3Object: {
        Bucket: eventBridgeS3Event.bucket,
        Name: eventBridgeS3Event.object,
      },
    },
  });

  // Textract returns a list of blocks. A block can be a line, a page, word, etc.
  // Each block also contains geometry of the detected text.
  // For more information on the Block type, see https://docs.aws.amazon.com/
textract/latest/dg/API_Block.html.
  const { Blocks } = await textractClient.send(detectDocumentTextCommand);

  // For the purpose of this example, we are only interested in words.
  const extractedWords = Blocks.filter((b) => b.BlockType === "WORD").map(
    (b) => b.Text,
  );

  return extractedWords.join(" ");
};
```

```
import { PollyClient, SynthesizeSpeechCommand } from "@aws-sdk/client-polly";
import { S3Client } from "@aws-sdk/client-s3";
import { Upload } from "@aws-sdk/lib-storage";

/**
 * Synthesize an audio file from text.
 *
 * @param {{ bucket: string, translated_text: string, object: string}}
 sourceDestinationConfig
 */
```

```
export const handler = async (sourceDestinationConfig) => {
  const pollyClient = new PollyClient({});

  const synthesizeSpeechCommand = new SynthesizeSpeechCommand({
    Engine: "neural",
    Text: sourceDestinationConfig.translated_text,
    VoiceId: "Ruth",
    OutputFormat: "mp3",
  });

  const { AudioStream } = await pollyClient.send(synthesizeSpeechCommand);

  const audioKey = `${sourceDestinationConfig.object}.mp3`;

  // Store the audio file in S3.
  const s3Client = new S3Client();
  const upload = new Upload({
    client: s3Client,
    params: {
      Bucket: sourceDestinationConfig.bucket,
      Key: audioKey,
      Body: AudioStream,
      ContentType: "audio/mp3",
    },
  });

  await upload.done();
  return audioKey;
};
```

```
import {
  TranslateClient,
  TranslateTextCommand,
} from "@aws-sdk/client-translate";

/**
 * Translate the extracted text to English.
 *
 * @param {{ extracted_text: string, source_language_code: string}}
 textAndSourceLanguage
 */
export const handler = async (textAndSourceLanguage) => {
  const translateClient = new TranslateClient({});
```

```
  const translateCommand = new TranslateTextCommand({
    SourceLanguageCode: textAndSourceLanguage.source_language_code,
    TargetLanguageCode: "en",
    Text: textAndSourceLanguage.extracted_text,
  });

  const { TranslatedText } = await translateClient.send(translateCommand);

  return { translated_text: TranslatedText };
};
```

Les services utilisés dans cet exemple

- Amazon Comprehend
- Lambda
- Amazon Polly
- Amazon Textract
- Amazon Translate

Ruby

Kit SDK pour Ruby

Cet exemple d'application analyse et stocke les cartes de commentaires des clients. Plus précisément, elle répond aux besoins d'un hôtel fictif situé à New York. L'hôtel reçoit les commentaires des clients dans différentes langues sous la forme de cartes de commentaires physiques. Ces commentaires sont chargés dans l'application via un client Web. Après avoir chargé l'image d'une carte de commentaires, les étapes suivantes se déroulent :

- Le texte est extrait de l'image à l'aide d'Amazon Textract.
- Amazon Comprehend détermine le sentiment du texte extrait et sa langue.
- Le texte extrait est traduit en anglais à l'aide d'Amazon Translate.
- Amazon Polly synthétise un fichier audio à partir du texte extrait.

L'application complète peut être déployée avec AWS CDK. Pour le code source et les instructions de déploiement, consultez le projet dans GitHub.

Les services utilisés dans cet exemple

- Amazon Comprehend

- Lambda
- Amazon Polly
- Amazon Textract
- Amazon Translate

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Création d'un tableau de bord de surveillance avec le nom de fonction comme variable

L'exemple de code suivant illustre comment :

- Créez un CloudWatch tableau de bord
- Ajouter des widgets de métriques Lambda avec une variable de nom de fonction
- Vérifier le tableau de bord
- nettoyer des ressources ;

Bash

AWS CLI avec le script Bash

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code.

```
#!/bin/bash

# Script to create a CloudWatch dashboard with Lambda function name as a variable
# This script creates a CloudWatch dashboard that allows you to switch between
 different Lambda functions

# Set up logging with secure permissions
LOG_FILE="${HOME}/.cloudwatch-dashboard-script.log"
```

```
touch "$LOG_FILE" && chmod 600 "$LOG_FILE"
exec > >(tee -a "$LOG_FILE") 2>&1

echo "$(date): Starting CloudWatch dashboard creation script"

# Security: Set strict error handling
set -uo pipefail
trap 'handle_error "Script failed at line $LINENO"' ERR

# Function to handle errors
handle_error() {
    local error_msg="${1:-Unknown error}"
    echo "ERROR: $error_msg" >&2
    echo "Resources created:"
    echo "- CloudWatch Dashboard: LambdaMetricsDashboard"
    echo ""
    echo "=========================================="
    echo "CLEANUP CONFIRMATION"
    echo "=========================================="
    echo "An error occurred. Proceeding with automatic cleanup..."

    echo "Cleaning up resources..."
    aws cloudwatch delete-dashboards --dashboard-names LambdaMetricsDashboard 2>/
dev/null || true

    # Clean up temporary files
    if [ -n "${TEMP_DIR:-}" ] && [ -d "$TEMP_DIR" ]; then
        rm -rf "$TEMP_DIR"
    fi
    rm -f dashboard-body.json

    echo "Cleanup complete."
    exit 1
}

# Security: Validate AWS CLI is installed
if ! command -v aws &> /dev/null; then
    handle_error "AWS CLI is not installed. Please install it and try again."
fi

# Check if AWS CLI is installed and configured
echo "Checking AWS CLI configuration..."
if ! aws sts get-caller-identity > /dev/null 2>&1; then
```

```
    handle_error "AWS CLI is not properly configured. Please configure it with
 'aws configure' and try again."
fi

# Get the current region securely
REGION=$(aws configure get region 2>/dev/null || echo "")
if [ -z "$REGION" ]; then
    REGION="us-east-1"
    echo "No region found in AWS config, defaulting to $REGION"
fi
echo "Using region: $REGION"

# Validate region format
if ! [[ "$REGION" =~ ^[a-z]{2}-[a-z]+-[0-9]{1}$ ]]; then
    handle_error "Invalid AWS region format: $REGION"
fi

# Check if there are any Lambda functions in the account
echo "Checking for Lambda functions..."
LAMBDA_FUNCTIONS=$(aws lambda list-functions --region "$REGION" --query
 "Functions[*].FunctionName" --output text 2>/dev/null || echo "")

if [ -z "$LAMBDA_FUNCTIONS" ]; then
    echo "No Lambda functions found in your account. Creating a simple test
 function..."

    # Create a temporary directory for Lambda function code with secure
 permissions
    TEMP_DIR=$(mktemp -d)
    chmod 700 "$TEMP_DIR"
    trap 'rm -rf "$TEMP_DIR"' EXIT

    # Create a simple Lambda function
    cat > "$TEMP_DIR/index.js" << 'EOF'
exports.handler = async (event) => {
    console.log('Event:', JSON.stringify(event, null, 2));
    return {
        statusCode: 200,
        body: JSON.stringify('Hello from Lambda!'),
    };
};
EOF

    # Zip the function code
```

```
    if ! cd "$TEMP_DIR"; then
        handle_error "Failed to change to temporary directory"
    fi

    if ! zip -q function.zip index.js; then
        handle_error "Failed to create zip file"
    fi

    # Create a role for the Lambda function with restricted trust policy
    ROLE_NAME="LambdaDashboardTestRole-$(date +%s)"
    TRUST_POLICY='{"Version":"2012-10-17",       "Statement":
[{"Effect":"Allow","Principal":
{"Service":"lambda.amazonaws.com"},"Action":"sts:AssumeRole"}]}'

    if ! ROLE_ARN=$(aws iam create-role \
        --role-name "$ROLE_NAME" \
        --assume-role-policy-document "$TRUST_POLICY" \
        --tags Key=project,Value=doc-smith Key=tutorial,Value=cloudwatch-
dynamicdash \
        --query "Role.Arn" \
        --output text 2>/dev/null); then
        handle_error "Failed to create IAM role for Lambda function"
    fi

    echo "Waiting for role to be available..."
    sleep 10

    # Attach basic Lambda execution policy
    if ! aws iam attach-role-policy \
        --role-name "$ROLE_NAME" \
        --policy-arn "arn:aws:iam::aws:policy/service-role/
AWSLambdaBasicExecutionRole"; then
        aws iam delete-role --role-name "$ROLE_NAME" 2>/dev/null || true
        handle_error "Failed to attach policy to IAM role"
    fi

    # Create the Lambda function
    FUNCTION_NAME="DashboardTestFunction-$(date +%s)"
    if ! aws lambda create-function \
        --function-name "$FUNCTION_NAME" \
        --runtime nodejs18.x \
        --role "$ROLE_ARN" \
        --handler index.handler \
        --zip-file fileb://function.zip \
```

```
        --tags project=doc-smith,tutorial=cloudwatch-dynamicdash \
        --region "$REGION" > /dev/null 2>&1; then
        aws iam detach-role-policy \
            --role-name "$ROLE_NAME" \
            --policy-arn "arn:aws:iam::aws:policy/service-role/
AWSLambdaBasicExecutionRole" 2>/dev/null || true
        aws iam delete-role --role-name "$ROLE_NAME" 2>/dev/null || true
        handle_error "Failed to create Lambda function"
    fi

    # Invoke the function to generate some metrics
    echo "Invoking Lambda function to generate metrics..."
    for i in {1..5}; do
        aws lambda invoke --function-name "$FUNCTION_NAME" --payload '{}' /dev/
null --region "$REGION" > /dev/null 2>&1 || true
        sleep 1
    done

    # Go back to original directory
    cd - > /dev/null

    # Set the function name for the dashboard
    DEFAULT_FUNCTION="$FUNCTION_NAME"
else
    # Use the first Lambda function as default
    DEFAULT_FUNCTION=$(echo "$LAMBDA_FUNCTIONS" | awk '{print $1}')
    echo "Found Lambda functions. Using $DEFAULT_FUNCTION as default."
    FUNCTION_NAME=""
    ROLE_NAME=""
fi

# Create a dashboard with Lambda metrics and a function name variable
echo "Creating CloudWatch dashboard with Lambda function name variable..."

# Create a JSON file for the dashboard body with secure permissions
DASHBOARD_JSON="dashboard-body-$$.json"
touch "$DASHBOARD_JSON" && chmod 600 "$DASHBOARD_JSON"

# Escape special characters in region and function name for JSON
REGION_ESCAPED=$(printf '%s\n' "$REGION" | sed 's:[\/&]:\\&:g')
FUNCTION_ESCAPED=$(printf '%s\n' "$DEFAULT_FUNCTION" | sed 's:[\/&]:\\&:g')

cat > "$DASHBOARD_JSON" << EOF
{
```

```
 "widgets": [
   {
     "type": "metric",
     "x": 0,
     "y": 0,
     "width": 12,
     "height": 6,
     "properties": {
       "metrics": [
         [ "AWS/Lambda", "Invocations", "FunctionName", "\${FunctionName}" ],
         [ ".", "Errors", ".", "." ],
         [ ".", "Throttles", ".", "." ]
       ],
       "view": "timeSeries",
       "stacked": false,
       "region": "$REGION_ESCAPED",
       "title": "Lambda Function Metrics for \${FunctionName}",
       "period": 300
     }
   },
   {
     "type": "metric",
     "x": 0,
     "y": 6,
     "width": 12,
     "height": 6,
     "properties": {
       "metrics": [
         [ "AWS/Lambda", "Duration", "FunctionName", "\${FunctionName}",
{ "stat": "Average" } ]
       ],
       "view": "timeSeries",
       "stacked": false,
       "region": "$REGION_ESCAPED",
       "title": "Duration for \${FunctionName}",
       "period": 300
     }
   },
   {
     "type": "metric",
     "x": 12,
     "y": 0,
     "width": 12,
     "height": 6,
```

```
      "properties": {
        "metrics": [
          [ "AWS/Lambda", "ConcurrentExecutions", "FunctionName", "\
${FunctionName}" ]
        ],
        "view": "timeSeries",
        "stacked": false,
        "region": "$REGION_ESCAPED",
        "title": "Concurrent Executions for \${FunctionName}",
        "period": 300
      }
    }
  ],
  "periodOverride": "auto",
  "variables": [
    {
      "type": "property",
      "id": "FunctionName",
      "property": "FunctionName",
      "label": "Lambda Function",
      "inputType": "select",
      "values": [
        {
          "value": "$FUNCTION_ESCAPED",
          "label": "$FUNCTION_ESCAPED"
        }
      ]
    }
  ]
}
EOF

# Validate JSON before sending
if ! jq empty "$DASHBOARD_JSON" 2>/dev/null; then
    handle_error "Invalid JSON generated for dashboard"
fi

# Create the dashboard using the JSON file
DASHBOARD_NAME="LambdaMetricsDashboard-$(date +%s)"
if ! DASHBOARD_RESULT=$(aws cloudwatch put-dashboard \
    --dashboard-name "$DASHBOARD_NAME" \
    --dashboard-body file://"$DASHBOARD_JSON" \
    --region "$REGION" 2>&1); then
    # If we created resources, clean them up
```

```
    if [ -n "${FUNCTION_NAME:-}" ]; then
        aws lambda delete-function --function-name "$FUNCTION_NAME" --region
 "$REGION" 2>/dev/null || true
        aws iam detach-role-policy \
            --role-name "$ROLE_NAME" \
            --policy-arn "arn:aws:iam::aws:policy/service-role/
AWSLambdaBasicExecutionRole" 2>/dev/null || true
        aws iam delete-role --role-name "$ROLE_NAME" 2>/dev/null || true
    fi
    handle_error "Failed to create CloudWatch dashboard."
fi

# Display any validation messages but continue
if echo "$DASHBOARD_RESULT" | grep -q "DashboardValidationMessages"; then
    echo "Dashboard created with validation messages:"
    echo "$DASHBOARD_RESULT"
    echo "These validation messages are warnings and the dashboard should still
 function."
else
    echo "Dashboard created successfully!"
fi

# Verify the dashboard was created
echo "Verifying dashboard creation..."
if ! DASHBOARD_INFO=$(aws cloudwatch get-dashboard --dashboard-name
 "$DASHBOARD_NAME" --region "$REGION" 2>&1); then
    # If we created resources, clean them up
    if [ -n "${FUNCTION_NAME:-}" ]; then
        aws lambda delete-function --function-name "$FUNCTION_NAME" --region
 "$REGION" 2>/dev/null || true
        aws iam detach-role-policy \
            --role-name "$ROLE_NAME" \
            --policy-arn "arn:aws:iam::aws:policy/service-role/
AWSLambdaBasicExecutionRole" 2>/dev/null || true
        aws iam delete-role --role-name "$ROLE_NAME" 2>/dev/null || true
    fi
    handle_error "Failed to verify dashboard creation."
fi

echo "Dashboard verification successful!"
echo "Dashboard details:"
echo "$DASHBOARD_INFO"

# List all dashboards to confirm
```

```
echo "Listing all dashboards:"
if ! DASHBOARDS=$(aws cloudwatch list-dashboards --region "$REGION" 2>&1); then
    # If we created resources, clean them up
    if [ -n "${FUNCTION_NAME:-}" ]; then
        aws lambda delete-function --function-name "$FUNCTION_NAME" --region
 "$REGION" 2>/dev/null || true
        aws iam detach-role-policy \
            --role-name "$ROLE_NAME" \
            --policy-arn "arn:aws:iam::aws:policy/service-role/
AWSLambdaBasicExecutionRole" 2>/dev/null || true
        aws iam delete-role --role-name "$ROLE_NAME" 2>/dev/null || true
    fi
    handle_error "Failed to list dashboards."
fi
echo "$DASHBOARDS"

# Show instructions for accessing the dashboard
echo ""
echo "Dashboard created successfully! To access it:"
echo "1. Open the CloudWatch console at https://console.aws.amazon.com/
cloudwatch/"
echo "2. In the navigation pane, choose Dashboards"
echo "3. Select $DASHBOARD_NAME"
echo "4. You should see a dropdown menu labeled 'Lambda Function' at the top of
 the dashboard"
echo "5. Use this dropdown to select different Lambda functions and see their
 metrics"
echo ""

# Create a list of resources for cleanup
RESOURCES=("- CloudWatch Dashboard: $DASHBOARD_NAME")
if [ -n "${FUNCTION_NAME:-}" ]; then
    RESOURCES+=("- Lambda Function: $FUNCTION_NAME")
    RESOURCES+=("- IAM Role: $ROLE_NAME")
fi

# Prompt for cleanup with automatic yes
echo "==========================================="
echo "CLEANUP CONFIRMATION"
echo "==========================================="
echo "Resources created:"
for resource in "${RESOURCES[@]}"; do
    echo "$resource"
done
```

```
echo ""
echo "Proceeding with automatic cleanup..."

CLEANUP_CHOICE="y"

if [[ "${CLEANUP_CHOICE,,}" == "y" ]]; then
    echo "Cleaning up resources..."

    # Delete the dashboard
    if aws cloudwatch delete-dashboards --dashboard-names "$DASHBOARD_NAME" --
region "$REGION" 2>/dev/null; then
        echo "Dashboard deleted successfully."
    else
        echo "WARNING: Failed to delete dashboard. You may need to delete it
 manually."
    fi

    # If we created a Lambda function, delete it and its role
    if [ -n "${FUNCTION_NAME:-}" ]; then
        echo "Deleting Lambda function..."
        if aws lambda delete-function --function-name "$FUNCTION_NAME" --region
 "$REGION" 2>/dev/null; then
            echo "Lambda function deleted successfully."
        else
            echo "WARNING: Failed to delete Lambda function. You may need to
 delete it manually."
        fi

        echo "Detaching role policy..."
        if aws iam detach-role-policy \
            --role-name "$ROLE_NAME" \
            --policy-arn "arn:aws:iam::aws:policy/service-role/
AWSLambdaBasicExecutionRole" 2>/dev/null; then
            echo "Role policy detached successfully."
        else
            echo "WARNING: Failed to detach role policy. You may need to detach
 it manually."
        fi

        echo "Deleting IAM role..."
        if aws iam delete-role --role-name "$ROLE_NAME" 2>/dev/null; then
            echo "IAM role deleted successfully."
        else
```

```
            echo "WARNING: Failed to delete IAM role. You may need to delete it
 manually."
        fi
    fi

    # Clean up the JSON file
    rm -f "$DASHBOARD_JSON"

    echo "Cleanup complete."
fi

echo "Script completed successfully!"
```

- Pour plus de détails sur l'API, consultez les rubriques suivantes dans la Référence des commandes de l'AWS CLI .
  - AttachRolePolicy
  - CreateFunction
  - CreateRole
  - DeleteDashboards
  - DeleteFunction
  - DeleteRole
  - DetachRolePolicy
  - GetCallerIdentity
  - GetDashboard
  - Invoke
  - ListDashboards
  - ListFunctions
  - PutDashboard

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Création de votre première fonction sans serveur

L'exemple de code suivant illustre comment :

- Création d'un rôle IAM pour Lambda
- Créer un code de fonction
- Création d’une fonction Lambda
- Testez votre fonction Lambda
- nettoyer des ressources ;

Bash

AWS CLI avec le script Bash

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l’exemple complet et découvrez comment le configurer et l’exécuter dans le référentiel d’exemples de code.

```
#!/bin/bash
# AWS Lambda - Create Your First Function
# This script creates a Lambda function, invokes it with a test event,
# views CloudWatch logs, and cleans up all resources.
#
# Source: https://docs.aws.amazon.com/lambda/latest/dg/getting-started.html
#
# Resources created:
#   - IAM role (Lambda execution role with basic logging permissions)
#   - Lambda function (Python 3.13 or Node.js 22.x runtime)
#   - CloudWatch log group (created automatically by Lambda on invocation)

set -eE -o pipefail

################################################################################
# Setup
################################################################################

UNIQUE_ID=$(head -c 8 /dev/urandom | od -An -tx1 | tr -d ' ')
FUNCTION_NAME="my-lambda-function-${UNIQUE_ID}"
ROLE_NAME="lambda-execution-role-${UNIQUE_ID}"
LOG_GROUP_NAME="/aws/lambda/${FUNCTION_NAME}"

TEMP_DIR=$(mktemp -d)
```

```
readonly TEMP_DIR
LOG_FILE="${TEMP_DIR}/lambda-gettingstarted.log"

exec > >(tee -a "$LOG_FILE") 2>&1

declare -a CREATED_RESOURCES

################################################################################
# Helper functions
################################################################################

cleanup_resources() {
    # Disable error trap to prevent recursion during cleanup
    trap - ERR
    set +eE

    echo ""
    echo "Cleaning up resources..."
    echo ""

    for ((i=${#CREATED_RESOURCES[@]}-1; i>=0; i--)); do
        local RESOURCE="${CREATED_RESOURCES[$i]}"
        local TYPE="${RESOURCE%%:*}"
        local NAME="${RESOURCE#*:}"

        case "$TYPE" in
            log-group)
                echo "Deleting CloudWatch log group: ${NAME}"
                aws logs delete-log-group \
                    --log-group-name "$NAME" 2>&1 || echo "  WARNING: Could not
 delete log group ${NAME}."
                ;;
            lambda-function)
                echo "Deleting Lambda function: ${NAME}"
                aws lambda delete-function \
                    --function-name "$NAME" 2>&1 || echo "  WARNING: Could not
 delete Lambda function ${NAME}."
                echo "  Waiting for function deletion to complete..."
                local DELETE_WAIT=0
                while aws lambda get-function --function-name "$NAME" > /dev/null
 2>&1; do
                    sleep 2
                    DELETE_WAIT=$((DELETE_WAIT + 2))
                    if [ "$DELETE_WAIT" -ge 60 ]; then
```

```
                        echo "  WARNING: Timed out waiting for function
 deletion."
                        break
                    fi
                done
                ;;
            iam-role-policy)
                local ROLE_PART="${NAME%%|*}"
                local POLICY_PART="${NAME#*|}"
                echo "Detaching policy from role: ${ROLE_PART}"
                aws iam detach-role-policy \
                    --role-name "$ROLE_PART" \
                    --policy-arn "$POLICY_PART" 2>&1 || echo "  WARNING: Could
 not detach policy from role ${ROLE_PART}."
                ;;
            iam-role)
                echo "Deleting IAM role: ${NAME}"
                aws iam delete-role \
                    --role-name "$NAME" 2>&1 || echo "  WARNING: Could not delete
 IAM role ${NAME}."
                ;;
        esac
    done

    if [ -d "$TEMP_DIR" ]; then
        rm -rf "$TEMP_DIR"
    fi

    echo ""
    echo "Cleanup complete."
}

handle_error() {
    echo ""
    echo "========================================="
    echo "ERROR: Script failed at $1"
    echo "========================================="
    echo ""
    if [ ${#CREATED_RESOURCES[@]} -gt 0 ]; then
        echo "Attempting to clean up ${#CREATED_RESOURCES[@]} resource(s)..."
        cleanup_resources
    fi
    exit 1
}
```

```
trap 'handle_error "line $LINENO"' ERR

wait_for_resource() {
    local DESCRIPTION="$1"
    local COMMAND="$2"
    local TARGET_VALUE="$3"
    local TIMEOUT=300
    local ELAPSED=0
    local INTERVAL=5

    echo "Waiting for ${DESCRIPTION}..."
    while true; do
        local RESULT
        RESULT=$(eval "$COMMAND" 2>&1) || true
        if echo "$RESULT" | grep -q "$TARGET_VALUE"; then
            echo "  ${DESCRIPTION} is ready."
            return 0
        fi
        if [ "$ELAPSED" -ge "$TIMEOUT" ]; then
            echo "ERROR: Timed out waiting for ${DESCRIPTION} after ${TIMEOUT}
 seconds."
            return 1
        fi
        sleep "$INTERVAL"
        ELAPSED=$((ELAPSED + INTERVAL))
    done
}

validate_input() {
    local input="$1"
    local pattern="$2"
    if ! [[ "$input" =~ $pattern ]]; then
        echo "ERROR: Invalid input: $input"
        return 1
    fi
    return 0
}

################################################################################
# Region pre-check
################################################################################

CONFIGURED_REGION=$(aws configure get region 2>/dev/null || true)
```

```
if [ -z "$CONFIGURED_REGION" ] && [ -z "$AWS_DEFAULT_REGION" ] && [ -z
 "$AWS_REGION" ]; then
    echo "ERROR: No AWS region configured."
    echo "Run 'aws configure set region <region>' or export AWS_DEFAULT_REGION."
    exit 1
fi

################################################################################
# Runtime selection
################################################################################

echo ""
echo "=========================================="
echo "AWS Lambda - Create Your First Function"
echo "=========================================="
echo ""
echo "Select a runtime for your Lambda function:"
echo "  1) Python 3.13"
echo "  2) Node.js 22.x"
echo ""
echo "Using default: Python 3.13"
RUNTIME_CHOICE="1"

case "$RUNTIME_CHOICE" in
    1)
        RUNTIME="python3.13"
        HANDLER="lambda_function.lambda_handler"
        CODE_FILE="lambda_function.py"
        cat > "${TEMP_DIR}/${CODE_FILE}" << 'PYTHON_EOF'
import json
import logging
logger = logging.getLogger()
logger.setLevel(logging.INFO)
def lambda_handler(event, context):
    if not isinstance(event, dict) or 'length' not in event or 'width' not in
 event:
        raise ValueError('Event must contain length and width')
    try:
        length = float(event['length'])
        width = float(event['width'])
        if length < 0 or width < 0:
            raise ValueError('Length and width must be non-negative')
        area = calculate_area(length, width)
        print(f'The area is {area}')
```

```
        logger.info(f'CloudWatch logs group: {context.log_group_name}')
        return json.dumps({'area': area})
    except (TypeError, ValueError) as e:
        logger.error(f'Error processing input: {str(e)}')
        raise
def calculate_area(length, width):
    return length * width
PYTHON_EOF
        echo "Selected runtime: Python 3.13"
        ;;
    2)
        RUNTIME="nodejs22.x"
        HANDLER="index.handler"
        CODE_FILE="index.mjs"
        cat > "${TEMP_DIR}/${CODE_FILE}" << 'NODEJS_EOF'
export const handler = async (event, context) => {
  if (!event || typeof event.length !== 'number' || typeof event.width !==
 'number') {
    throw new Error('Event must contain numeric length and width');
  }
  if (event.length < 0 || event.width < 0) {
    throw new Error('Length and width must be non-negative');
  }
  const area = event.length * event.width;
  console.log(`The area is ${area}`);
  console.log('CloudWatch log group: ', context.logGroupName);
  return JSON.stringify({area});
};
NODEJS_EOF
        echo "Selected runtime: Node.js 22.x"
        ;;
    *)
        echo "ERROR: Invalid choice. Please enter 1 or 2."
        exit 1
        ;;
esac

# ============================================================================
# Step 1: Create IAM execution role
# ============================================================================

echo ""
echo "=========================================="
echo "Step 1: Create IAM execution role"
```

```
echo "========================================="
echo ""

TRUST_POLICY='{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "lambda.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}'

echo "Creating IAM role: ${ROLE_NAME}"
ROLE_OUTPUT=$(aws iam create-role \
    --role-name "$ROLE_NAME" \
    --assume-role-policy-document "$TRUST_POLICY" \
    --query 'Role.Arn' \
    --output text 2>&1)

if ! validate_input "$ROLE_OUTPUT" "^arn:aws:iam::[0-9]+:role/"; then
    echo "ERROR: Failed to create IAM role"
    exit 1
fi

echo "$ROLE_OUTPUT"
ROLE_ARN="$ROLE_OUTPUT"
CREATED_RESOURCES+=("iam-role:${ROLE_NAME}")
echo "Role ARN: ${ROLE_ARN}"

aws iam tag-role \
    --role-name "$ROLE_NAME" \
    --tags Key=project,Value=doc-smith Key=tutorial,Value=lambda-gettingstarted

echo ""
echo "Attaching AWSLambdaBasicExecutionRole policy..."
aws iam attach-role-policy \
    --role-name "$ROLE_NAME" \
    --policy-arn "arn:aws:iam::aws:policy/service-role/
AWSLambdaBasicExecutionRole" 2>&1
```

```
CREATED_RESOURCES+=("iam-role-policy:${ROLE_NAME}|arn:aws:iam::aws:policy/
service-role/AWSLambdaBasicExecutionRole")
echo "Policy attached."

# IAM roles can take a few seconds to propagate
echo "Waiting for IAM role to propagate..."
sleep 10

################################################################################
# Step 2: Create Lambda function
################################################################################

echo ""
echo "========================================="
echo "Step 2: Create Lambda function"
echo "========================================="
echo ""

echo "Creating deployment package..."
ORIGINAL_DIR=$(pwd)
cd "$TEMP_DIR" || exit 1
zip -j function.zip "$CODE_FILE" > /dev/null 2>&1 || {
    echo "ERROR: Failed to create deployment package"
    exit 1
}
cd "$ORIGINAL_DIR" || exit 1

if [ ! -f "${TEMP_DIR}/function.zip" ]; then
    echo "ERROR: Deployment package creation failed"
    exit 1
fi

echo "Creating Lambda function: ${FUNCTION_NAME}"
echo "  Runtime: ${RUNTIME}"
echo "  Handler: ${HANDLER}"
echo ""

CREATE_OUTPUT=$(aws lambda create-function \
    --function-name "$FUNCTION_NAME" \
    --runtime "$RUNTIME" \
    --role "$ROLE_ARN" \
    --handler "$HANDLER" \
    --architectures x86_64 \
    --zip-file "fileb://${TEMP_DIR}/function.zip" \
```

```
    --tags project=doc-smith,tutorial=lambda-gettingstarted \
    --query '[FunctionName, FunctionArn, Runtime, State]' \
    --output text 2>&1)

if [ -z "$CREATE_OUTPUT" ]; then
    echo "ERROR: Failed to create Lambda function"
    exit 1
fi

echo "$CREATE_OUTPUT"
CREATED_RESOURCES+=("lambda-function:${FUNCTION_NAME}")

wait_for_resource "Lambda function to become Active" \
    "aws lambda get-function-configuration --function-name ${FUNCTION_NAME} --
query State --output text" \
    "Active"

###############################################################################
# Step 3: Invoke the function
###############################################################################

echo ""
echo "==========================================="
echo "Step 3: Invoke the function"
echo "==========================================="
echo ""

TEST_EVENT='{"length": 6, "width": 7}'
echo "Invoking function with test event: ${TEST_EVENT}"
echo ""

echo "$TEST_EVENT" > "${TEMP_DIR}/test-event.json"

if ! validate_input "$TEST_EVENT" '"length": [0-9]+, "width": [0-9]+'; then
    echo "ERROR: Invalid test event format"
    exit 1
fi

INVOKE_OUTPUT=$(aws lambda invoke \
    --function-name "$FUNCTION_NAME" \
    --payload "fileb://${TEMP_DIR}/test-event.json" \
    --cli-read-timeout 30 \
    "${TEMP_DIR}/response.json" 2>&1)
echo "$INVOKE_OUTPUT"
```

```
if [ ! -f "${TEMP_DIR}/response.json" ]; then
    echo "ERROR: No response file generated"
    exit 1
fi

RESPONSE=$(cat "${TEMP_DIR}/response.json")
echo ""
echo "Function response: ${RESPONSE}"
echo ""

if echo "$INVOKE_OUTPUT" | grep -qi "functionerror"; then
    echo "WARNING: Function returned an error."
fi

################################################################################
# Step 4: View CloudWatch logs
################################################################################

echo ""
echo "========================================="
echo "Step 4: View CloudWatch Logs"
echo "========================================="
echo ""

echo "Log group: ${LOG_GROUP_NAME}"
echo ""

echo "Waiting for CloudWatch logs to be available..."

LOG_STREAMS=""
for i in $(seq 1 6); do
    LOG_STREAMS=$(aws logs describe-log-streams \
        --log-group-name "$LOG_GROUP_NAME" \
        --order-by LastEventTime \
        --descending \
        --query 'logStreams[0].logStreamName' \
        --output text 2>/dev/null) || true
    if [ -n "$LOG_STREAMS" ] && [ "$LOG_STREAMS" != "None" ]; then
        break
    fi
    LOG_STREAMS=""
    sleep 5
done
```

```
if [ -n "$LOG_STREAMS" ] && [ "$LOG_STREAMS" != "None" ]; then
    echo "Latest log stream: ${LOG_STREAMS}"
    echo ""
    echo "--- Log events ---"
    LOG_EVENTS=$(aws logs get-log-events \
        --log-group-name "$LOG_GROUP_NAME" \
        --log-stream-name "$LOG_STREAMS" \
        --query 'events[].message' \
        --output text 2>&1) || true
    echo "$LOG_EVENTS"
    echo "--- End of log events ---"
else
    echo "No log streams found yet. Logs may take a moment to appear."
    echo "You can view them in the CloudWatch console:"
    echo "  Log group: ${LOG_GROUP_NAME}"
fi

CREATED_RESOURCES+=("log-group:${LOG_GROUP_NAME}")

aws logs tag-log-group \
    --log-group-name "$LOG_GROUP_NAME" \
    --tags project=doc-smith,tutorial=lambda-gettingstarted

################################################################################
# Summary and cleanup
################################################################################

echo ""
echo "========================================="
echo "SUMMARY"
echo "========================================="
echo ""
echo "Resources created:"
echo "  IAM role:          ${ROLE_NAME}"
echo "  Lambda function:   ${FUNCTION_NAME}"
echo "  CloudWatch logs:   ${LOG_GROUP_NAME}"
echo ""
echo "========================================="
echo "CLEANUP"
echo "========================================="
echo ""
echo "Cleaning up all created resources..."
cleanup_resources
```

```
echo ""
echo "Done."
```

- Pour plus de détails sur l'API, consultez les rubriques suivantes dans la Référence des commandes de l'AWS CLI .
  - AttachRolePolicy
  - CreateFunction
  - CreateRole
  - DeleteFunction
  - DeleteLogGroup
  - DeleteRole
  - DescribeLogStreams
  - DetachRolePolicy
  - GetFunction
  - GetFunctionConfiguration
  - GetLogEvents
  - Invoke

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Invoquer une fonction Lambda à partir d'un navigateur

L'exemple de code suivant montre comment invoquer un AWS Lambda fonction depuis un navigateur.

JavaScript

SDK pour JavaScript (version 2)

Vous pouvez créer une application basée sur un navigateur qui utilise un AWS Lambda fonction permettant de mettre à jour une table Amazon DynamoDB avec les sélections de l'utilisateur.

Pour le code source complet et les instructions de configuration et d'exécution, consultez l'exemple complet sur GitHub.

Les services utilisés dans cet exemple

- DynamoDB
- Lambda

SDK pour JavaScript (v3)

Vous pouvez créer une application basée sur un navigateur qui utilise un AWS Lambda fonction permettant de mettre à jour une table Amazon DynamoDB avec les sélections de l'utilisateur. Cette application utilise AWS SDK pour JavaScript v3.

Pour le code source complet et les instructions de configuration et d'exécution, consultez l'exemple complet sur GitHub.

Les services utilisés dans cet exemple

- DynamoDB
- Lambda

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Transformation des données pour votre application avec S3 Object Lambda

L'exemple de code suivant illustre comment transformer des données pour votre application avec S3 Object Lambda.

.NET

SDK pour .NET

Explique comment ajouter du code personnalisé aux requêtes GET S3 standard afin de modifier l'objet demandé extrait de S3 pour qu'il réponde aux besoins du client ou de l'application qui le demande.

Pour le code source complet et les instructions de configuration et d'exécution, consultez l'exemple complet sur GitHub.

Les services utilisés dans cet exemple

- Lambda
- Amazon S3

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Utiliser API Gateway pour invoquer une fonction Lambda

Les exemples de code suivants montrent comment créer un AWS Lambda fonction invoquée par Amazon API Gateway.

Java

SDK pour Java 2.x

Montre comment créer un AWS Lambda fonction à l'aide de l'API d'exécution Java Lambda. Cet exemple invoque différents AWS services pour réaliser un cas d'utilisation spécifique. Cet exemple montre comment créer une fonction Lambda invoquée par Amazon API Gateway qui analyse une table Amazon DynamoDB à la recherche d’anniversaires professionnels et utilise Amazon Simple Notification Service (Amazon SNS) pour envoyer un message texte à vos employés qui les félicitent à leur date d’anniversaire.

Pour le code source complet et les instructions de configuration et d'exécution, consultez l'exemple complet sur GitHub.

Les services utilisés dans cet exemple

- API Gateway
- DynamoDB
- Lambda
- Amazon SNS

JavaScript

SDK pour JavaScript (v3)

Montre comment créer un AWS Lambda fonction à l'aide du Lambda JavaScript API d'exécution. Cet exemple invoque différents AWS services pour réaliser un cas d'utilisation spécifique. Cet exemple montre comment créer une fonction Lambda invoquée par Amazon API Gateway qui analyse une table Amazon DynamoDB à la recherche d'anniversaires professionnels et utilise Amazon Simple Notification Service (Amazon SNS) pour envoyer un message texte à vos employés qui les félicitent à leur date d'anniversaire.

Pour le code source complet et les instructions de configuration et d'exécution, consultez l'exemple complet sur GitHub.

Cet exemple est également disponible dans le AWS SDK pour JavaScript guide du développeur v3.

Les services utilisés dans cet exemple

- API Gateway
- DynamoDB
- Lambda
- Amazon SNS

Python

Kit SDK for Python (Boto3)

Cet exemple montre comment créer et utiliser une API REST Amazon API Gateway qui cible une fonction AWS Lambda . Le gestionnaire Lambda explique comment router en fonction des méthodes HTTP, comment obtenir des données à partir de la chaîne de requête, de l'en-tête et du corps, et comment renvoyer une réponse JSON.

- Déployer une fonction Lambda.
- Créer une API REST avec API Gateway.
- Créer une ressource REST qui cible la fonction Lambda.
- Accorder à API Gateway l'autorisation d'invoquer la fonction Lambda.
- Utiliser le package Requests (Requêtes) pour envoyer des requêtes à l'API REST.

- Nettoyer toutes les ressources créées lors de la démonstration.

Il est préférable de visionner cet exemple sur GitHub. Pour le code source complet et les instructions de configuration et d'exécution, consultez l'exemple complet sur GitHub.

Les services utilisés dans cet exemple

- API Gateway
- DynamoDB
- Lambda
- Amazon SNS

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Utiliser les fonctions Step Functions pour invoquer des fonctions Lambda

L'exemple de code suivant montre comment créer un AWS Step Functions machine à états qui invoque AWS Lambda fonctions en séquence.

Java

SDK pour Java 2.x

Montre comment créer un AWS flux de travail sans serveur en utilisant AWS Step Functions et le AWS SDK for Java 2.x. Chaque étape du flux de travail est mise en œuvre à l'aide d'un AWS Lambda fonction.

Pour le code source complet et les instructions de configuration et d'exécution, consultez l'exemple complet sur GitHub.

Les services utilisés dans cet exemple

- DynamoDB
- Lambda
- Amazon SES
- Fonctions de l'étape

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Utilisent des événements planifiés pour invoquer une fonction Lambda

Les exemples de code suivants montrent comment créer un AWS Lambda fonction invoquée par un Amazon EventBridge événement programmé.

Java

SDK pour Java 2.x

Montre comment créer un Amazon EventBridge événement planifié qui invoque un AWS Lambda fonction. Configurez EventBridge pour utiliser une expression cron pour planifier l'appel de la fonction Lambda. Dans cet exemple, vous créez une fonction Lambda à l'aide de l'API d'exécution Lambda. Cet exemple invoque différents AWS services pour réaliser un cas d'utilisation spécifique. Cet exemple montre comment créer une application qui envoie un message texte mobile à vos employés pour les féliciter à leur date d'anniversaire.

Pour le code source complet et les instructions de configuration et d'exécution, consultez l'exemple complet sur GitHub.

Les services utilisés dans cet exemple

- CloudWatch Journaux
- DynamoDB
- EventBridge
- Lambda
- Amazon SNS

JavaScript

SDK pour JavaScript (v3)

Montre comment créer un Amazon EventBridge événement planifié qui invoque un AWS Lambda fonction. Configurez EventBridge pour utiliser une expression cron pour planifier l'appel de la fonction Lambda. Dans cet exemple, vous créez une fonction Lambda à l'aide du Lambda JavaScript API d'exécution. Cet exemple invoque différents AWS services pour

réaliser un cas d'utilisation spécifique. Cet exemple montre comment créer une application qui envoie un message texte mobile à vos employés pour les féliciter à leur date d'anniversaire.

Pour le code source complet et les instructions de configuration et d'exécution, consultez l'exemple complet sur GitHub.

Cet exemple est également disponible dans le AWS SDK pour JavaScript guide du développeur v3.

Les services utilisés dans cet exemple

- CloudWatch Journaux
- DynamoDB
- EventBridge
- Lambda
- Amazon SNS

Python

Kit SDK for Python (Boto3)

Cet exemple montre comment enregistrer un AWS Lambda fonctionner en tant que cible d'un Amazon planifié EventBridge événement. Le gestionnaire Lambda écrit un message convivial et les données complètes de l'événement à Amazon CloudWatch Journaux pour une récupération ultérieure.

- Déploie une fonction Lambda.
- Crée un EventBridge événement planifié et fait de la fonction Lambda la cible.
- Octroie l'autorisation de louer EventBridge invoquez la fonction Lambda.
- Imprime les données les plus récentes de CloudWatch Journaux pour afficher le résultat des appels planifiés.
- Nettoie toutes les ressources créées lors de la démonstration.

Il est préférable de visionner cet exemple sur GitHub. Pour le code source complet et les instructions de configuration et d'exécution, consultez l'exemple complet sur GitHub.

Les services utilisés dans cet exemple

- CloudWatch Journaux
- DynamoDB

- EventBridge
- Lambda
- Amazon SNS

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Utiliser l'API Amazon Neptune pour développer une fonction Lambda qui interroge les données d'un graphe

L'exemple de code suivant montre comment utiliser l'API Neptune pour interroger les données d'un graphe.

Java

SDK pour Java 2.x

Montre comment utiliser l'API Java Amazon Neptune pour créer une fonction Lambda qui interroge les données de graphe au sein du VPC.

Pour le code source complet et les instructions de configuration et d'exécution, consultez l'exemple complet sur GitHub.

Les services utilisés dans cet exemple

- Lambda
- Neptune

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Utilisation de variables de propriété dans les tableaux de bord de surveillance pour surveiller plusieurs fonctions sans serveur

L'exemple de code suivant illustre comment :

- Créer des fonctions Lambda pour la surveillance

- Créez un CloudWatch tableau de bord
- Ajouter une variable de propriété au tableau de bord
- nettoyer des ressources ;

Bash

AWS CLI avec le script Bash

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code.

```
#!/bin/bash

# CloudWatch Dashboard with Lambda Function Variable Script
# This script creates a CloudWatch dashboard with a property variable for Lambda
 function names

set -euo pipefail

# Security: Set restrictive umask
umask 0077

# Set up logging with secure permissions
LOG_FILE="cloudwatch-dashboard-script-v4.log"
touch "$LOG_FILE"
chmod 600 "$LOG_FILE"
echo "Starting script execution at $(date)" >> "$LOG_FILE"

# Function to log commands and their output (with sensitive data sanitization)
log_cmd() {
    local cmd="$1"
    local sanitized_cmd="${cmd//--password*/--password [REDACTED]}"
    sanitized_cmd="${sanitized_cmd//--secret*/--secret [REDACTED]}"
    echo "$(date): Running command: $sanitized_cmd" >> "$LOG_FILE"
    eval "$cmd" 2>&1 | tee -a "$LOG_FILE"
    return ${PIPESTATUS[0]}
}
```

```
# Function to check for errors in command output
check_error() {
    local cmd_output="$1"
    local cmd_status="$2"
    local error_msg="$3"

    if [ $cmd_status -ne 0 ] || echo "$cmd_output" | grep -qi "error"; then
        echo "ERROR: $error_msg" | tee -a "$LOG_FILE"
        # Sanitize output before logging
        local sanitized_output="${cmd_output//arn:aws:iam::[0-9]*/
arn:aws:iam::ACCOUNT_ID}"
        echo "Command output: $sanitized_output" | tee -a "$LOG_FILE"
        cleanup_resources
        exit 1
    fi
}

# Trap errors and cleanup
trap 'cleanup_resources' EXIT ERR INT TERM

# Function to clean up resources
cleanup_resources() {
    local exit_code=$?

    echo "" | tee -a "$LOG_FILE"
    echo "========================================" | tee -a "$LOG_FILE"
    echo "CLEANUP PROCESS" | tee -a "$LOG_FILE"
    echo "========================================" | tee -a "$LOG_FILE"

    if [ -n "${DASHBOARD_NAME:-}" ]; then
        echo "Deleting CloudWatch dashboard: $DASHBOARD_NAME" | tee -a
 "$LOG_FILE"
        aws cloudwatch delete-dashboards --dashboard-names "$DASHBOARD_NAME" 2>&1
 >> "$LOG_FILE" || true
    fi

    if [ -n "${LAMBDA_FUNCTION1:-}" ]; then
        echo "Deleting Lambda function: $LAMBDA_FUNCTION1" | tee -a "$LOG_FILE"
        aws lambda delete-function --function-name "$LAMBDA_FUNCTION1" 2>&1 >>
 "$LOG_FILE" || true
    fi

    if [ -n "${LAMBDA_FUNCTION2:-}" ]; then
        echo "Deleting Lambda function: $LAMBDA_FUNCTION2" | tee -a "$LOG_FILE"
```

```
        aws lambda delete-function --function-name "$LAMBDA_FUNCTION2" 2>&1 >>
 "$LOG_FILE" || true
    fi

    if [ -n "${ROLE_NAME:-}" ]; then
        echo "Detaching policy from role: $ROLE_NAME" | tee -a "$LOG_FILE"
        aws iam detach-role-policy --role-name "$ROLE_NAME" --policy-arn
 arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole 2>&1 >>
 "$LOG_FILE" || true

        echo "Deleting IAM role: $ROLE_NAME" | tee -a "$LOG_FILE"
        aws iam delete-role --role-name "$ROLE_NAME" 2>&1 >> "$LOG_FILE" || true
    fi

    # Clean up temporary files securely
    shred -vfz -n 3 trust-policy.json lambda_function.py lambda_function.zip 2>/
dev/null || rm -f trust-policy.json lambda_function.py lambda_function.zip

    echo "Cleanup completed." | tee -a "$LOG_FILE"

    return $exit_code
}

# Validate AWS CLI is installed and authenticated
if ! command -v aws &> /dev/null; then
    echo "ERROR: AWS CLI is not installed" | tee -a "$LOG_FILE"
    exit 1
fi

if ! aws sts get-caller-identity &> /dev/null; then
    echo "ERROR: AWS CLI is not properly authenticated" | tee -a "$LOG_FILE"
    exit 1
fi

# Get AWS region with validation
AWS_REGION=$(aws configure get region 2>/dev/null || echo "")
if [ -z "$AWS_REGION" ]; then
    AWS_REGION="us-east-1"
    echo "No region found in AWS config, defaulting to $AWS_REGION" | tee -a
 "$LOG_FILE"
else
    echo "Using AWS region: $AWS_REGION" | tee -a "$LOG_FILE"
fi
```

```
# Validate region format
if ! [[ "$AWS_REGION" =~ ^[a-z]{2}-[a-z]+-[0-9]$ ]]; then
    echo "ERROR: Invalid AWS region format: $AWS_REGION" | tee -a "$LOG_FILE"
    exit 1
fi

# Generate unique identifiers using secure random with validation
RANDOM_ID=$(openssl rand -hex 6)
if [ -z "$RANDOM_ID" ] || [ ${#RANDOM_ID} -ne 12 ]; then
    echo "ERROR: Failed to generate valid random identifier" | tee -a "$LOG_FILE"
    exit 1
fi

DASHBOARD_NAME="LambdaMetricsDashboard-${RANDOM_ID}"
LAMBDA_FUNCTION1="TestFunction1-${RANDOM_ID}"
LAMBDA_FUNCTION2="TestFunction2-${RANDOM_ID}"
ROLE_NAME="LambdaExecutionRole-${RANDOM_ID}"

# Validate resource names don't exceed AWS limits
if [ ${#DASHBOARD_NAME} -gt 128 ] || [ ${#LAMBDA_FUNCTION1} -gt 64 ] ||
 [ ${#ROLE_NAME} -gt 64 ]; then
    echo "ERROR: Generated resource names exceed AWS limits" | tee -a "$LOG_FILE"
    exit 1
fi

echo "Using random identifier: $RANDOM_ID" | tee -a "$LOG_FILE"
echo "Dashboard name: $DASHBOARD_NAME" | tee -a "$LOG_FILE"
echo "Lambda function names: $LAMBDA_FUNCTION1, $LAMBDA_FUNCTION2" | tee -a
 "$LOG_FILE"
echo "IAM role name: $ROLE_NAME" | tee -a "$LOG_FILE"

# Create IAM role for Lambda functions
echo "Creating IAM role for Lambda..." | tee -a "$LOG_FILE"
TRUST_POLICY='{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
```

```
}'

echo "$TRUST_POLICY" > trust-policy.json
chmod 600 trust-policy.json

# Validate JSON before use
if ! python3 -m json.tool trust-policy.json > /dev/null 2>&1; then
    echo "ERROR: Invalid trust policy JSON" | tee -a "$LOG_FILE"
    exit 1
fi

ROLE_OUTPUT=$(log_cmd "aws iam create-role --role-name '$ROLE_NAME' --assume-
role-policy-document file://trust-policy.json --tags Key=project,Value=doc-smith
 Key=tutorial,Value=cloudwatch-streams --output json")
check_error "$ROLE_OUTPUT" $? "Failed to create IAM role"

ROLE_ARN=$(echo "$ROLE_OUTPUT" | python3 -c "import sys, json;
 print(json.load(sys.stdin)['Role']['Arn'])" 2>/dev/null)
if [ -z "$ROLE_ARN" ]; then
    echo "ERROR: Failed to extract Role ARN" | tee -a "$LOG_FILE"
    exit 1
fi
echo "Role ARN: $ROLE_ARN" | tee -a "$LOG_FILE"

# Attach Lambda basic execution policy to the role
echo "Attaching Lambda execution policy to role..." | tee -a "$LOG_FILE"
POLICY_OUTPUT=$(log_cmd "aws iam attach-role-policy --role-name '$ROLE_NAME' --
policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole")
check_error "$POLICY_OUTPUT" $? "Failed to attach policy to role"

# Wait for role to propagate
echo "Waiting for IAM role to propagate..." | tee -a "$LOG_FILE"
sleep 10

# Create simple Python Lambda function code with security validation
echo "Creating Lambda function code..." | tee -a "$LOG_FILE"
cat > lambda_function.py << 'LAMBDA_EOF'
def handler(event, context):
    print("Lambda function executed successfully")
    return {
        'statusCode': 200,
        'body': 'Success'
    }
LAMBDA_EOF
```

```
chmod 600 lambda_function.py

# Validate Python syntax
if ! python3 -m py_compile lambda_function.py 2>/dev/null; then
    echo "ERROR: Invalid Python syntax in Lambda function" | tee -a "$LOG_FILE"
    exit 1
fi

# Zip the Lambda function code
zip -j -q lambda_function.zip lambda_function.py
if [ ! -f lambda_function.zip ]; then
    echo "ERROR: Failed to create lambda_function.zip" | tee -a "$LOG_FILE"
    exit 1
fi
chmod 600 lambda_function.zip

# Validate zip file integrity
if ! unzip -t lambda_function.zip > /dev/null 2>&1; then
    echo "ERROR: Created zip file is corrupted" | tee -a "$LOG_FILE"
    exit 1
fi

# Create first Lambda function
echo "Creating first Lambda function: $LAMBDA_FUNCTION1..." | tee -a "$LOG_FILE"
LAMBDA1_OUTPUT=$(log_cmd "aws lambda create-function --function-name
 '$LAMBDA_FUNCTION1' --runtime python3.11 --role '$ROLE_ARN' --handler
 lambda_function.handler --zip-file fileb://lambda_function.zip --timeout 30 --
memory-size 128 --tags project=doc-smith,tutorial=cloudwatch-streams")
check_error "$LAMBDA1_OUTPUT" $? "Failed to create first Lambda function"

# Create second Lambda function
echo "Creating second Lambda function: $LAMBDA_FUNCTION2..." | tee -a "$LOG_FILE"
LAMBDA2_OUTPUT=$(log_cmd "aws lambda create-function --function-name
 '$LAMBDA_FUNCTION2' --runtime python3.11 --role '$ROLE_ARN' --handler
 lambda_function.handler --zip-file fileb://lambda_function.zip --timeout 30 --
memory-size 128 --tags project=doc-smith,tutorial=cloudwatch-streams")
check_error "$LAMBDA2_OUTPUT" $? "Failed to create second Lambda function"

# Invoke Lambda functions to generate some metrics
echo "Invoking Lambda functions to generate metrics..." | tee -a "$LOG_FILE"
log_cmd "aws lambda invoke --function-name '$LAMBDA_FUNCTION1' --payload '{}' /
dev/null" || true
```

```
log_cmd "aws lambda invoke --function-name '$LAMBDA_FUNCTION2' --payload '{}' /
dev/null" || true

# Create CloudWatch dashboard with property variable
echo "Creating CloudWatch dashboard with property variable..." | tee -a
 "$LOG_FILE"

# Create dashboard body with proper escaping and validation
DASHBOARD_BODY=$(cat <<EOF
{
  "widgets": [
    {
      "type": "metric",
      "x": 0,
      "y": 0,
      "width": 12,
      "height": 6,
      "properties": {
        "metrics": [
          [ "AWS/Lambda", "Invocations", "FunctionName", "$LAMBDA_FUNCTION1" ]
        ],
        "view": "timeSeries",
        "stacked": false,
        "region": "$AWS_REGION",
        "title": "Lambda Invocations",
        "period": 300,
        "stat": "Sum"
      }
    }
  ]
}
EOF
)

# Validate JSON before sending
if ! echo "$DASHBOARD_BODY" | python3 -m json.tool > /dev/null 2>&1; then
    echo "ERROR: Dashboard body is not valid JSON" | tee -a "$LOG_FILE"
    exit 1
fi

# First create a basic dashboard without variables
echo "Creating initial dashboard without variables..." | tee -a "$LOG_FILE"
DASHBOARD_OUTPUT=$(aws cloudwatch put-dashboard --dashboard-name
 "$DASHBOARD_NAME" --dashboard-body "$DASHBOARD_BODY" --output json 2>&1)
```

```
check_error "$DASHBOARD_OUTPUT" $? "Failed to create initial CloudWatch
 dashboard"

# Now let's try to add a property variable using the console instructions
echo "To complete the tutorial, please follow these steps in the CloudWatch
 console:" | tee -a "$LOG_FILE"
echo "1. Open the CloudWatch console at https://console.aws.amazon.com/
cloudwatch/" | tee -a "$LOG_FILE"
echo "2. Navigate to Dashboards and select your dashboard: $DASHBOARD_NAME" | tee
 -a "$LOG_FILE"
echo "3. Choose Actions > Variables > Create a variable" | tee -a "$LOG_FILE"
echo "4. Choose Property variable" | tee -a "$LOG_FILE"
echo "5. For Property that the variable changes, choose FunctionName" | tee -a
 "$LOG_FILE"
echo "6. For Input type, choose Select menu (dropdown)" | tee -a "$LOG_FILE"
echo "7. Choose Use the results of a metric search" | tee -a "$LOG_FILE"
echo "8. Choose Pre-built queries > Lambda > Errors" | tee -a "$LOG_FILE"
echo "9. Choose By Function Name and then choose Search" | tee -a "$LOG_FILE"
echo "10. (Optional) Configure any secondary settings as desired" | tee -a
 "$LOG_FILE"
echo "11. Choose Add variable" | tee -a "$LOG_FILE"
echo "" | tee -a "$LOG_FILE"
echo "The dashboard has been created and can be accessed at:" | tee -a
 "$LOG_FILE"
echo "https://console.aws.amazon.com/cloudwatch/home#dashboards:name=
$DASHBOARD_NAME" | tee -a "$LOG_FILE"

# Verify dashboard creation
echo "Verifying dashboard creation..." | tee -a "$LOG_FILE"
VERIFY_OUTPUT=$(aws cloudwatch get-dashboard --dashboard-name "$DASHBOARD_NAME"
 --output json 2>&1)
check_error "$VERIFY_OUTPUT" $? "Failed to verify dashboard creation"

echo "" | tee -a "$LOG_FILE"
echo "==========================================" | tee -a "$LOG_FILE"
echo "DASHBOARD CREATED SUCCESSFULLY" | tee -a "$LOG_FILE"
echo "==========================================" | tee -a "$LOG_FILE"
echo "Dashboard Name: $DASHBOARD_NAME" | tee -a "$LOG_FILE"
echo "Lambda Functions: $LAMBDA_FUNCTION1, $LAMBDA_FUNCTION2" | tee -a
 "$LOG_FILE"
echo "" | tee -a "$LOG_FILE"
echo "You can view your dashboard in the CloudWatch console:" | tee -a
 "$LOG_FILE"
```

```
echo "https://console.aws.amazon.com/cloudwatch/home#dashboards:name=
$DASHBOARD_NAME" | tee -a "$LOG_FILE"
echo "" | tee -a "$LOG_FILE"

# Auto-confirm cleanup
echo "" | tee -a "$LOG_FILE"
echo "========================================" | tee -a "$LOG_FILE"
echo "CLEANUP CONFIRMATION" | tee -a "$LOG_FILE"
echo "========================================" | tee -a "$LOG_FILE"
echo "The following resources were created:" | tee -a "$LOG_FILE"
echo "- CloudWatch Dashboard: $DASHBOARD_NAME" | tee -a "$LOG_FILE"
echo "- Lambda Function: $LAMBDA_FUNCTION1" | tee -a "$LOG_FILE"
echo "- Lambda Function: $LAMBDA_FUNCTION2" | tee -a "$LOG_FILE"
echo "- IAM Role: $ROLE_NAME" | tee -a "$LOG_FILE"
echo "" | tee -a "$LOG_FILE"
echo "Auto-confirming cleanup of all created resources..." | tee -a "$LOG_FILE"

echo "Script completed successfully." | tee -a "$LOG_FILE"
exit 0
```

- Pour plus de détails sur l'API, consultez les rubriques suivantes dans la Référence des commandes de l'AWS CLI .
  - AttachRolePolicy
  - CreateFunction
  - CreateRole
  - DeleteDashboards
  - DeleteFunction
  - DeleteRole
  - DetachRolePolicy
  - GetDashboard
  - Invoke
  - PutDashboard

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Écrivez des données d'activité personnalisées à l'aide d'une fonction Lambda après l'authentification utilisateur Amazon Cognito à l'aide d'un AWS Kit SDK

L'exemple de code suivant illustre comment écrire des données d'activité personnalisées avec une fonction Lambda après l'authentification utilisateur Amazon Cognito.

- Utilisez les fonctions d'administrateur pour ajouter un utilisateur à un groupe d'utilisateurs.
- Configurez un groupe d'utilisateurs pour appeler une fonction Lambda pour le déclencheur `PostAuthentication`.
- Inscrivez le nouvel utilisateur dans Amazon Cognito.
- La fonction Lambda écrit des informations personnalisées dans CloudWatch Enregistre et dans une table DynamoDB.
- Obtenez et affichez les données personnalisées à partir de la table DynamoDB, puis nettoyer les ressources.

Go

Kit SDK pour Go V2

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Exécutez un scénario interactif à une invite de commande.

```
import (
 "context"
 "errors"
 "log"
 "strings"
 "user_pools_and_lambda_triggers/actions"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/service/cognitoidentityprovider"
```

```
 "github.com/aws/aws-sdk-go-v2/service/cognitoidentityprovider/types"
 "github.com/awsdocs/aws-doc-sdk-examples/gov2/demotools"
)

// ActivityLog separates the steps of this scenario into individual functions so
 that
// they are simpler to read and understand.
type ActivityLog struct {
 helper       IScenarioHelper
 questioner   demotools.IQuestioner
 resources    Resources
 cognitoActor *actions.CognitoActions
}

// NewActivityLog constructs a new activity log runner.
func NewActivityLog(sdkConfig aws.Config, questioner demotools.IQuestioner,
 helper IScenarioHelper) ActivityLog {
 scenario := ActivityLog{
  helper:       helper,
  questioner:   questioner,
  resources:    Resources{},
  cognitoActor: &actions.CognitoActions{CognitoClient:
 cognitoidentityprovider.NewFromConfig(sdkConfig)},
 }
 scenario.resources.init(scenario.cognitoActor, questioner)
 return scenario
}

// AddUserToPool selects a user from the known users table and uses administrator
 credentials to add the user to the user pool.
func (runner *ActivityLog) AddUserToPool(ctx context.Context, userPoolId string,
 tableName string) (string, string) {
 log.Println("To facilitate this example, let's add a user to the user pool using
 administrator privileges.")
 users, err := runner.helper.GetKnownUsers(ctx, tableName)
 if err != nil {
  panic(err)
 }
 user := users.Users[0]
 log.Printf("Adding known user %v to the user pool.\n", user.UserName)
 err = runner.cognitoActor.AdminCreateUser(ctx, userPoolId, user.UserName,
 user.UserEmail)
 if err != nil {
  panic(err)
```

```
 }
 pwSet := false
 password := runner.questioner.AskPassword("\nEnter a password that has at least
 eight characters, uppercase, lowercase, numbers and symbols.\n"+
  "(the password will not display as you type):", 8)
 for !pwSet {
  log.Printf("\nSetting password for user '%v'.\n", user.UserName)
  err = runner.cognitoActor.AdminSetUserPassword(ctx, userPoolId, user.UserName,
 password)
  if err != nil {
   var invalidPassword *types.InvalidPasswordException
   if errors.As(err, &invalidPassword) {
    password = runner.questioner.AskPassword("\nEnter another password:", 8)
   } else {
    panic(err)
   }
  } else {
   pwSet = true
  }
 }

 log.Println(strings.Repeat("-", 88))

 return user.UserName, password
}

// AddActivityLogTrigger adds a Lambda handler as an invocation target for the
 PostAuthentication trigger.
func (runner *ActivityLog) AddActivityLogTrigger(ctx context.Context, userPoolId
 string, activityLogArn string) {
 log.Println("Let's add a Lambda function to handle the PostAuthentication
 trigger from Cognito.\n" +
  "This trigger happens after a user is authenticated, and lets your function
 take action, such as logging\n" +
  "the outcome.")
 err := runner.cognitoActor.UpdateTriggers(
  ctx, userPoolId,
  actions.TriggerInfo{Trigger: actions.PostAuthentication, HandlerArn:
 aws.String(activityLogArn)})
 if err != nil {
  panic(err)
 }
 runner.resources.triggers = append(runner.resources.triggers,
 actions.PostAuthentication)
```

```
 log.Printf("Lambda function %v added to user pool %v to handle
 PostAuthentication Cognito trigger.\n",
  activityLogArn, userPoolId)

 log.Println(strings.Repeat("-", 88))
}

// SignInUser signs in as the specified user.
func (runner *ActivityLog) SignInUser(ctx context.Context, clientId string,
 userName string, password string) {
 log.Printf("Now we'll sign in user %v and check the results in the logs and the
 DynamoDB table.", userName)
 runner.questioner.Ask("Press Enter when you're ready.")
 authResult, err := runner.cognitoActor.SignIn(ctx, clientId, userName, password)
 if err != nil {
  panic(err)
 }
 log.Println("Sign in successful.",
  "The PostAuthentication Lambda handler writes custom information to CloudWatch
 Logs.")

 runner.resources.userAccessTokens = append(runner.resources.userAccessTokens,
 *authResult.AccessToken)
}

// GetKnownUserLastLogin gets the login info for a user from the Amazon DynamoDB
 table and displays it.
func (runner *ActivityLog) GetKnownUserLastLogin(ctx context.Context, tableName
 string, userName string) {
 log.Println("The PostAuthentication handler also writes login data to the
 DynamoDB table.")
 runner.questioner.Ask("Press Enter when you're ready to continue.")
 users, err := runner.helper.GetKnownUsers(ctx, tableName)
 if err != nil {
  panic(err)
 }
 for _, user := range users.Users {
  if user.UserName == userName {
   log.Println("The last login info for the user in the known users table is:")
   log.Printf("\t%+v", *user.LastLogin)
  }
 }
 log.Println(strings.Repeat("-", 88))
}
```

```
// Run runs the scenario.
func (runner *ActivityLog) Run(ctx context.Context, stackName string) {
 defer func() {
  if r := recover(); r != nil {
   log.Println("Something went wrong with the demo.")
   runner.resources.Cleanup(ctx)
  }
 }()

 log.Println(strings.Repeat("-", 88))
 log.Printf("Welcome\n")

 log.Println(strings.Repeat("-", 88))

 stackOutputs, err := runner.helper.GetStackOutputs(ctx, stackName)
 if err != nil {
  panic(err)
 }
 runner.resources.userPoolId = stackOutputs["UserPoolId"]
 runner.helper.PopulateUserTable(ctx, stackOutputs["TableName"])
 userName, password := runner.AddUserToPool(ctx, stackOutputs["UserPoolId"],
 stackOutputs["TableName"])

 runner.AddActivityLogTrigger(ctx, stackOutputs["UserPoolId"],
 stackOutputs["ActivityLogFunctionArn"])
 runner.SignInUser(ctx, stackOutputs["UserPoolClientId"], userName, password)
 runner.helper.ListRecentLogEvents(ctx, stackOutputs["ActivityLogFunction"])
 runner.GetKnownUserLastLogin(ctx, stackOutputs["TableName"], userName)

 runner.resources.Cleanup(ctx)

 log.Println(strings.Repeat("-", 88))
 log.Println("Thanks for watching!")
 log.Println(strings.Repeat("-", 88))
}
```

Gérez le déclencheur `PostAuthentication` avec une fonction Lambda.

```
import (
```

```
 "context"
 "fmt"
 "log"
 "os"
 "time"

 "github.com/aws/aws-lambda-go/events"
 "github.com/aws/aws-lambda-go/lambda"
 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/config"
 "github.com/aws/aws-sdk-go-v2/feature/dynamodb/attributevalue"
 "github.com/aws/aws-sdk-go-v2/service/dynamodb"
 dynamodbtypes "github.com/aws/aws-sdk-go-v2/service/dynamodb/types"
)

const TABLE_NAME = "TABLE_NAME"

// LoginInfo defines structured login data that can be marshalled to a DynamoDB
 format.
type LoginInfo struct {
 UserPoolId string `dynamodbav:"UserPoolId"`
 ClientId   string `dynamodbav:"ClientId"`
 Time       string `dynamodbav:"Time"`
}

// UserInfo defines structured user data that can be marshalled to a DynamoDB
 format.
type UserInfo struct {
 UserName  string    `dynamodbav:"UserName"`
 UserEmail string    `dynamodbav:"UserEmail"`
 LastLogin LoginInfo `dynamodbav:"LastLogin"`
}

// GetKey marshals the user email value to a DynamoDB key format.
func (user UserInfo) GetKey() map[string]dynamodbtypes.AttributeValue {
 userEmail, err := attributevalue.Marshal(user.UserEmail)
 if err != nil {
  panic(err)
 }
 return map[string]dynamodbtypes.AttributeValue{"UserEmail": userEmail}
}

type handler struct {
 dynamoClient *dynamodb.Client
```

```
}

// HandleRequest handles the PostAuthentication event by writing custom data to
 the logs and
// to an Amazon DynamoDB table.
func (h *handler) HandleRequest(ctx context.Context,
 event events.CognitoEventUserPoolsPostAuthentication)
 (events.CognitoEventUserPoolsPostAuthentication, error) {
 log.Printf("Received post authentication trigger from %v for user '%v'",
 event.TriggerSource, event.UserName)
 tableName := os.Getenv(TABLE_NAME)
 user := UserInfo{
  UserName:  event.UserName,
  UserEmail: event.Request.UserAttributes["email"],
  LastLogin: LoginInfo{
   UserPoolId: event.UserPoolID,
   ClientId:   event.CallerContext.ClientID,
   Time:       time.Now().Format(time.UnixDate),
  },
 }
 // Write to CloudWatch Logs.
 fmt.Printf("%#v", user)

 // Also write to an external system. This examples uses DynamoDB to demonstrate.
 userMap, err := attributevalue.MarshalMap(user)
 if err != nil {
  log.Printf("Couldn't marshal to DynamoDB map. Here's why: %v\n", err)
 } else if len(userMap) == 0 {
  log.Printf("User info marshaled to an empty map.")
 } else {
  _, err := h.dynamoClient.PutItem(ctx, &dynamodb.PutItemInput{
   Item:      userMap,
   TableName: aws.String(tableName),
  })
  if err != nil {
   log.Printf("Couldn't write to DynamoDB. Here's why: %v\n", err)
  } else {
   log.Printf("Wrote user info to DynamoDB table %v.\n", tableName)
  }
 }

 return event, nil
}
```

```
func main() {
 ctx := context.Background()
 sdkConfig, err := config.LoadDefaultConfig(ctx)
 if err != nil {
  log.Panicln(err)
 }
 h := handler{
  dynamoClient: dynamodb.NewFromConfig(sdkConfig),
 }
 lambda.Start(h.HandleRequest)
}
```

Créez une structure qui exécute les tâches courantes.

```
import (
 "context"
 "log"
 "strings"
 "time"
 "user_pools_and_lambda_triggers/actions"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/service/cloudformation"
 "github.com/aws/aws-sdk-go-v2/service/cloudwatchlogs"
 "github.com/aws/aws-sdk-go-v2/service/dynamodb"
 "github.com/awsdocs/aws-doc-sdk-examples/gov2/demotools"
)

// IScenarioHelper defines common functions used by the workflows in this
 example.
type IScenarioHelper interface {
 Pause(secs int)
 GetStackOutputs(ctx context.Context, stackName string) (actions.StackOutputs,
 error)
 PopulateUserTable(ctx context.Context, tableName string)
 GetKnownUsers(ctx context.Context, tableName string) (actions.UserList, error)
 AddKnownUser(ctx context.Context, tableName string, user actions.User)
 ListRecentLogEvents(ctx context.Context, functionName string)
}
```

```
// ScenarioHelper contains AWS wrapper structs used by the workflows in this
 example.
type ScenarioHelper struct {
 questioner  demotools.IQuestioner
 dynamoActor *actions.DynamoActions
 cfnActor    *actions.CloudFormationActions
 cwlActor    *actions.CloudWatchLogsActions
 isTestRun   bool
}

// NewScenarioHelper constructs a new scenario helper.
func NewScenarioHelper(sdkConfig aws.Config, questioner demotools.IQuestioner)
 ScenarioHelper {
 scenario := ScenarioHelper{
  questioner:  questioner,
  dynamoActor: &actions.DynamoActions{DynamoClient:
 dynamodb.NewFromConfig(sdkConfig)},
  cfnActor:    &actions.CloudFormationActions{CfnClient:
 cloudformation.NewFromConfig(sdkConfig)},
  cwlActor:    &actions.CloudWatchLogsActions{CwlClient:
 cloudwatchlogs.NewFromConfig(sdkConfig)},
 }
 return scenario
}

// Pause waits for the specified number of seconds.
func (helper ScenarioHelper) Pause(secs int) {
 if !helper.isTestRun {
  time.Sleep(time.Duration(secs) * time.Second)
 }
}

// GetStackOutputs gets the outputs from the specified CloudFormation stack in a
 structured format.
func (helper ScenarioHelper) GetStackOutputs(ctx context.Context, stackName
 string) (actions.StackOutputs, error) {
 return helper.cfnActor.GetOutputs(ctx, stackName), nil
}

// PopulateUserTable fills the known user table with example data.
func (helper ScenarioHelper) PopulateUserTable(ctx context.Context, tableName
 string) {
 log.Printf("First, let's add some users to the DynamoDB %v table we'll use for
 this example.\n", tableName)
```

```
 err := helper.dynamoActor.PopulateTable(ctx, tableName)
 if err != nil {
  panic(err)
 }
}

// GetKnownUsers gets the users from the known users table in a structured
 format.
func (helper ScenarioHelper) GetKnownUsers(ctx context.Context, tableName string)
 (actions.UserList, error) {
 knownUsers, err := helper.dynamoActor.Scan(ctx, tableName)
 if err != nil {
  log.Printf("Couldn't get known users from table %v. Here's why: %v\n",
 tableName, err)
 }
 return knownUsers, err
}

// AddKnownUser adds a user to the known users table.
func (helper ScenarioHelper) AddKnownUser(ctx context.Context, tableName string,
 user actions.User) {
 log.Printf("Adding user '%v' with email '%v' to the DynamoDB known users
 table...\n",
  user.UserName, user.UserEmail)
 err := helper.dynamoActor.AddUser(ctx, tableName, user)
 if err != nil {
  panic(err)
 }
}

// ListRecentLogEvents gets the most recent log stream and events for the
 specified Lambda function and displays them.
func (helper ScenarioHelper) ListRecentLogEvents(ctx context.Context,
 functionName string) {
 log.Println("Waiting a few seconds to let Lambda write to CloudWatch Logs...")
 helper.Pause(10)
 log.Println("Okay, let's check the logs to find what's happened recently with
 your Lambda function.")
 logStream, err := helper.cwlActor.GetLatestLogStream(ctx, functionName)
 if err != nil {
  panic(err)
 }
 log.Printf("Getting some recent events from log stream %v\n",
 *logStream.LogStreamName)
```

```
 events, err := helper.cwlActor.GetLogEvents(ctx, functionName,
 *logStream.LogStreamName, 10)
 if err != nil {
  panic(err)
 }
 for _, event := range events {
  log.Printf("\t%v", *event.Message)
 }
 log.Println(strings.Repeat("-", 88))
}
```

Créez une structure qui encapsule les actions Amazon Cognito.

```
import (
 "context"
 "errors"
 "log"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/service/cognitoidentityprovider"
 "github.com/aws/aws-sdk-go-v2/service/cognitoidentityprovider/types"
)

type CognitoActions struct {
 CognitoClient *cognitoidentityprovider.Client
}



// Trigger and TriggerInfo define typed data for updating an Amazon Cognito
 trigger.
type Trigger int

const (
 PreSignUp Trigger = iota
 UserMigration
 PostAuthentication
)

type TriggerInfo struct {
```

```
 Trigger    Trigger
 HandlerArn *string
}

// UpdateTriggers adds or removes Lambda triggers for a user pool. When a trigger
 is specified with a `nil` value,
// it is removed from the user pool.
func (actor CognitoActions) UpdateTriggers(ctx context.Context, userPoolId
 string, triggers ...TriggerInfo) error {
 output, err := actor.CognitoClient.DescribeUserPool(ctx,
 &cognitoidentityprovider.DescribeUserPoolInput{
  UserPoolId: aws.String(userPoolId),
 })
 if err != nil {
  log.Printf("Couldn't get info about user pool %v. Here's why: %v\n",
 userPoolId, err)
  return err
 }
 lambdaConfig := output.UserPool.LambdaConfig
 for _, trigger := range triggers {
  switch trigger.Trigger {
  case PreSignUp:
   lambdaConfig.PreSignUp = trigger.HandlerArn
  case UserMigration:
   lambdaConfig.UserMigration = trigger.HandlerArn
  case PostAuthentication:
   lambdaConfig.PostAuthentication = trigger.HandlerArn
  }
 }
 _, err = actor.CognitoClient.UpdateUserPool(ctx,
 &cognitoidentityprovider.UpdateUserPoolInput{
  UserPoolId:   aws.String(userPoolId),
  LambdaConfig: lambdaConfig,
 })
 if err != nil {
  log.Printf("Couldn't update user pool %v. Here's why: %v\n", userPoolId, err)
 }
 return err
}



// SignUp signs up a user with Amazon Cognito.
```

```
func (actor CognitoActions) SignUp(ctx context.Context, clientId string, userName
 string, password string, userEmail string) (bool, error) {
 confirmed := false
 output, err := actor.CognitoClient.SignUp(ctx,
 &cognitoidentityprovider.SignUpInput{
  ClientId: aws.String(clientId),
  Password: aws.String(password),
  Username: aws.String(userName),
  UserAttributes: []types.AttributeType{
   {Name: aws.String("email"), Value: aws.String(userEmail)},
  },
 })
 if err != nil {
  var invalidPassword *types.InvalidPasswordException
  if errors.As(err, &invalidPassword) {
   log.Println(*invalidPassword.Message)
  } else {
   log.Printf("Couldn't sign up user %v. Here's why: %v\n", userName, err)
  }
 } else {
  confirmed = output.UserConfirmed
 }
 return confirmed, err
}



// SignIn signs in a user to Amazon Cognito using a username and password
 authentication flow.
func (actor CognitoActions) SignIn(ctx context.Context, clientId string, userName
 string, password string) (*types.AuthenticationResultType, error) {
 var authResult *types.AuthenticationResultType
 output, err := actor.CognitoClient.InitiateAuth(ctx,
 &cognitoidentityprovider.InitiateAuthInput{
  AuthFlow:       "USER_PASSWORD_AUTH",
  ClientId:       aws.String(clientId),
  AuthParameters: map[string]string{"USERNAME": userName, "PASSWORD": password},
 })
 if err != nil {
  var resetRequired *types.PasswordResetRequiredException
  if errors.As(err, &resetRequired) {
   log.Println(*resetRequired.Message)
  } else {
   log.Printf("Couldn't sign in user %v. Here's why: %v\n", userName, err)
```

```
  }
 } else {
  authResult = output.AuthenticationResult
 }
 return authResult, err
}



// ForgotPassword starts a password recovery flow for a user. This flow typically
 sends a confirmation code
// to the user's configured notification destination, such as email.
func (actor CognitoActions) ForgotPassword(ctx context.Context, clientId string,
 userName string) (*types.CodeDeliveryDetailsType, error) {
 output, err := actor.CognitoClient.ForgotPassword(ctx,
 &cognitoidentityprovider.ForgotPasswordInput{
  ClientId: aws.String(clientId),
  Username: aws.String(userName),
 })
 if err != nil {
  log.Printf("Couldn't start password reset for user '%v'. Here;s why: %v\n",
 userName, err)
 }
 return output.CodeDeliveryDetails, err
}



// ConfirmForgotPassword confirms a user with a confirmation code and a new
 password.
func (actor CognitoActions) ConfirmForgotPassword(ctx context.Context, clientId
 string, code string, userName string, password string) error {
 _, err := actor.CognitoClient.ConfirmForgotPassword(ctx,
 &cognitoidentityprovider.ConfirmForgotPasswordInput{
  ClientId:         aws.String(clientId),
  ConfirmationCode: aws.String(code),
  Password:         aws.String(password),
  Username:         aws.String(userName),
 })
 if err != nil {
  var invalidPassword *types.InvalidPasswordException
  if errors.As(err, &invalidPassword) {
   log.Println(*invalidPassword.Message)
  } else {
```

```
   log.Printf("Couldn't confirm user %v. Here's why: %v", userName, err)
  }
 }
 return err
}



// DeleteUser removes a user from the user pool.
func (actor CognitoActions) DeleteUser(ctx context.Context, userAccessToken
 string) error {
 _, err := actor.CognitoClient.DeleteUser(ctx,
 &cognitoidentityprovider.DeleteUserInput{
  AccessToken: aws.String(userAccessToken),
 })
 if err != nil {
  log.Printf("Couldn't delete user. Here's why: %v\n", err)
 }
 return err
}



// AdminCreateUser uses administrator credentials to add a user to a user pool.
 This method leaves the user
// in a state that requires they enter a new password next time they sign in.
func (actor CognitoActions) AdminCreateUser(ctx context.Context, userPoolId
 string, userName string, userEmail string) error {
 _, err := actor.CognitoClient.AdminCreateUser(ctx,
 &cognitoidentityprovider.AdminCreateUserInput{
  UserPoolId:     aws.String(userPoolId),
  Username:       aws.String(userName),
  MessageAction:  types.MessageActionTypeSuppress,
  UserAttributes: []types.AttributeType{{Name: aws.String("email"), Value:
 aws.String(userEmail)}},
 })
 if err != nil {
  var userExists *types.UsernameExistsException
  if errors.As(err, &userExists) {
   log.Printf("User %v already exists in the user pool.", userName)
   err = nil
  } else {
   log.Printf("Couldn't create user %v. Here's why: %v\n", userName, err)
  }
```

```
 }
 return err
}



// AdminSetUserPassword uses administrator credentials to set a password for a
 user without requiring a
// temporary password.
func (actor CognitoActions) AdminSetUserPassword(ctx context.Context, userPoolId
 string, userName string, password string) error {
 _, err := actor.CognitoClient.AdminSetUserPassword(ctx,
 &cognitoidentityprovider.AdminSetUserPasswordInput{
  Password:   aws.String(password),
  UserPoolId: aws.String(userPoolId),
  Username:   aws.String(userName),
  Permanent:  true,
 })
 if err != nil {
  var invalidPassword *types.InvalidPasswordException
  if errors.As(err, &invalidPassword) {
   log.Println(*invalidPassword.Message)
  } else {
   log.Printf("Couldn't set password for user %v. Here's why: %v\n", userName,
 err)
  }
 }
 return err
}
```

Créez une structure qui encapsule les actions DynamoDB.

```
import (
 "context"
 "fmt"
 "log"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/feature/dynamodb/attributevalue"
 "github.com/aws/aws-sdk-go-v2/service/dynamodb"
```

```
 "github.com/aws/aws-sdk-go-v2/service/dynamodb/types"
)

// DynamoActions encapsulates the Amazon Simple Notification Service (Amazon SNS)
 actions
// used in the examples.
type DynamoActions struct {
 DynamoClient *dynamodb.Client
}

// User defines structured user data.
type User struct {
 UserName  string
 UserEmail string
 LastLogin *LoginInfo `dynamodbav:",omitempty"`
}

// LoginInfo defines structured custom login data.
type LoginInfo struct {
 UserPoolId string
 ClientId   string
 Time       string
}

// UserList defines a list of users.
type UserList struct {
 Users []User
}

// UserNameList returns the usernames contained in a UserList as a list of
 strings.
func (users *UserList) UserNameList() []string {
 names := make([]string, len(users.Users))
 for i := 0; i < len(users.Users); i++ {
  names[i] = users.Users[i].UserName
 }
 return names
}

// PopulateTable adds a set of test users to the table.
func (actor DynamoActions) PopulateTable(ctx context.Context, tableName string)
 error {
 var err error
 var item map[string]types.AttributeValue
```

```
 var writeReqs []types.WriteRequest
 for i := 1; i < 4; i++ {
  item, err = attributevalue.MarshalMap(User{UserName: fmt.Sprintf("test_user_
%v", i), UserEmail: fmt.Sprintf("test_email_%v@example.com", i)})
  if err != nil {
   log.Printf("Couldn't marshall user into DynamoDB format. Here's why: %v\n",
 err)
   return err
  }
  writeReqs = append(writeReqs, types.WriteRequest{PutRequest:
 &types.PutRequest{Item: item}})
 }
 _, err = actor.DynamoClient.BatchWriteItem(ctx, &dynamodb.BatchWriteItemInput{
  RequestItems: map[string][]types.WriteRequest{tableName: writeReqs},
 })
 if err != nil {
  log.Printf("Couldn't populate table %v with users. Here's why: %v\n",
 tableName, err)
 }
 return err
}

// Scan scans the table for all items.
func (actor DynamoActions) Scan(ctx context.Context, tableName string) (UserList,
 error) {
 var userList UserList
 output, err := actor.DynamoClient.Scan(ctx, &dynamodb.ScanInput{
  TableName: aws.String(tableName),
 })
 if err != nil {
  log.Printf("Couldn't scan table %v for items. Here's why: %v\n", tableName,
 err)
 } else {
  err = attributevalue.UnmarshalListOfMaps(output.Items, &userList.Users)
  if err != nil {
   log.Printf("Couldn't unmarshal items into users. Here's why: %v\n", err)
  }
 }
 return userList, err
}

// AddUser adds a user item to a table.
func (actor DynamoActions) AddUser(ctx context.Context, tableName string, user
 User) error {
```

```
 userItem, err := attributevalue.MarshalMap(user)
 if err != nil {
  log.Printf("Couldn't marshall user to item. Here's why: %v\n", err)
 }
 _, err = actor.DynamoClient.PutItem(ctx, &dynamodb.PutItemInput{
  Item:      userItem,
  TableName: aws.String(tableName),
 })
 if err != nil {
  log.Printf("Couldn't put item in table %v. Here's why: %v", tableName, err)
 }
 return err
}
```

Créez une structure qui enveloppe CloudWatch Enregistre les actions.

```
import (
 "context"
 "fmt"
 "log"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/service/cloudwatchlogs"
 "github.com/aws/aws-sdk-go-v2/service/cloudwatchlogs/types"
)

type CloudWatchLogsActions struct {
 CwlClient *cloudwatchlogs.Client
}

// GetLatestLogStream gets the most recent log stream for a Lambda function.
func (actor CloudWatchLogsActions) GetLatestLogStream(ctx context.Context,
 functionName string) (types.LogStream, error) {
 var logStream types.LogStream
 logGroupName := fmt.Sprintf("/aws/lambda/%s", functionName)
 output, err := actor.CwlClient.DescribeLogStreams(ctx,
 &cloudwatchlogs.DescribeLogStreamsInput{
  Descending:   aws.Bool(true),
  Limit:        aws.Int32(1),
  LogGroupName: aws.String(logGroupName),
```

```
  OrderBy:      types.OrderByLastEventTime,
 })
 if err != nil {
  log.Printf("Couldn't get log streams for log group %v. Here's why: %v\n",
 logGroupName, err)
 } else {
  logStream = output.LogStreams[0]
 }
 return logStream, err
}

// GetLogEvents gets the most recent eventCount events from the specified log
 stream.
func (actor CloudWatchLogsActions) GetLogEvents(ctx context.Context, functionName
 string, logStreamName string, eventCount int32) (
 []types.OutputLogEvent, error) {
 var events []types.OutputLogEvent
 logGroupName := fmt.Sprintf("/aws/lambda/%s", functionName)
 output, err := actor.CwlClient.GetLogEvents(ctx,
 &cloudwatchlogs.GetLogEventsInput{
  LogStreamName: aws.String(logStreamName),
  Limit:         aws.Int32(eventCount),
  LogGroupName:  aws.String(logGroupName),
 })
 if err != nil {
  log.Printf("Couldn't get log event for log stream %v. Here's why: %v\n",
 logStreamName, err)
 } else {
  events = output.Events
 }
 return events, err
}
```

Créez une structure qui enveloppe CloudFormation actions.

```
import (
 "context"
 "log"

 "github.com/aws/aws-sdk-go-v2/aws"
```

```
 "github.com/aws/aws-sdk-go-v2/service/cloudformation"
)

// StackOutputs defines a map of outputs from a specific stack.
type StackOutputs map[string]string

type CloudFormationActions struct {
 CfnClient *cloudformation.Client
}

// GetOutputs gets the outputs from a CloudFormation stack and puts them into a
 structured format.
func (actor CloudFormationActions) GetOutputs(ctx context.Context, stackName
 string) StackOutputs {
 output, err := actor.CfnClient.DescribeStacks(ctx,
 &cloudformation.DescribeStacksInput{
  StackName: aws.String(stackName),
 })
 if err != nil || len(output.Stacks) == 0 {
  log.Panicf("Couldn't find a CloudFormation stack named %v. Here's why: %v\n",
 stackName, err)
 }
 stackOutputs := StackOutputs{}
 for _, out := range output.Stacks[0].Outputs {
  stackOutputs[*out.OutputKey] = *out.OutputValue
 }
 return stackOutputs
}
```

Nettoyez les ressources.

```
import (
 "context"
 "log"
 "user_pools_and_lambda_triggers/actions"

 "github.com/awsdocs/aws-doc-sdk-examples/gov2/demotools"
)

// Resources keeps track of AWS resources created during an example and handles
```

```
// cleanup when the example finishes.
type Resources struct {
 userPoolId       string
 userAccessTokens []string
 triggers         []actions.Trigger

 cognitoActor *actions.CognitoActions
 questioner   demotools.IQuestioner
}

func (resources *Resources) init(cognitoActor *actions.CognitoActions, questioner
 demotools.IQuestioner) {
 resources.userAccessTokens = []string{}
 resources.triggers = []actions.Trigger{}
 resources.cognitoActor = cognitoActor
 resources.questioner = questioner
}

// Cleanup deletes all AWS resources created during an example.
func (resources *Resources) Cleanup(ctx context.Context) {
 defer func() {
  if r := recover(); r != nil {
   log.Printf("Something went wrong during cleanup.\n%v\n", r)
   log.Println("Use the AWS Management Console to remove any remaining resources
 \n" +
    "that were created for this scenario.")
  }
 }()

 wantDelete := resources.questioner.AskBool("Do you want to remove all of the AWS
 resources that were created "+
  "during this demo (y/n)?", "y")
 if wantDelete {
  for _, accessToken := range resources.userAccessTokens {
   err := resources.cognitoActor.DeleteUser(ctx, accessToken)
   if err != nil {
    log.Println("Couldn't delete user during cleanup.")
    panic(err)
   }
   log.Println("Deleted user.")
  }
  triggerList := make([]actions.TriggerInfo, len(resources.triggers))
  for i := 0; i < len(resources.triggers); i++ {
```

```
    triggerList[i] = actions.TriggerInfo{Trigger: resources.triggers[i],
  HandlerArn: nil}
   }
   err := resources.cognitoActor.UpdateTriggers(ctx, resources.userPoolId,
  triggerList...)
   if err != nil {
    log.Println("Couldn't update Cognito triggers during cleanup.")
    panic(err)
   }
   log.Println("Removed Cognito triggers from user pool.")
  } else {
   log.Println("Be sure to remove resources when you're done with them to avoid
  unexpected charges!")
  }
 }
```

- Pour plus de détails sur l'API, consultez les rubriques suivantes dans la Référence des API du kit AWS SDK pour Go .
  - AdminCreateUser
  - AdminSetUserPassword
  - DeleteUser
  - InitiateAuth
  - UpdateUserPool

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Exemples sans serveur pour Lambda

Les exemples de code suivants montrent comment utiliser Lambda avec AWS SDK.

Exemples

- Connexion à une base de données Amazon RDS dans une fonction Lambda
- Invoquer une fonction Lambda à partir d'un déclencheur Kinesis
- Invocation d'une fonction Lambda à partir d'un déclencheur DynamoDB

- Invocation d'une fonction Lambda à partir d'un déclencheur Amazon DocumentDB
- Invocation d'une fonction Lambda à partir d'un déclencheur Amazon MSK
- Invoquer une fonction Lambda à partir d'un déclencheur Amazon S3
- Invocation d'une fonction lambda à partir d'un déclencheur Amazon SNS
- Invoquer une fonction Lambda à partir d'un déclencheur Amazon SQS
- Signalement des échecs d'articles par lots pour les fonctions Lambda à l'aide d'un déclencheur Kinesis
- Signalement des échecs d'articles par lots pour les fonctions Lambda à l'aide d'un déclencheur DynamoDB
- Signalement des échecs d'articles par lots pour les fonctions Lambda à l'aide d'un déclencheur Amazon SQS

Connexion à une base de données Amazon RDS dans une fonction Lambda

Les exemples de code suivants illustrent comment implémenter une fonction Lambda qui se connecte à une base de données RDS. La fonction effectue une simple requête de base de données et renvoie le résultat.

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Connexion à une base de données Amazon RDS dans une fonction Lambda à l'aide de .NET.

```
using System.Data;
using System.Text.Json;
using Amazon.Lambda.APIGatewayEvents;
using Amazon.Lambda.Core;
using MySql.Data.MySqlClient;
```

```
// Assembly attribute to enable the Lambda function's JSON input to be converted
 into a .NET class.
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSeri

namespace aws_rds;

public class InputModel
{
    public string key1 { get; set; }
    public string key2 { get; set; }
}

public class Function
{
    /// <summary>
    // Handles the Lambda function execution for connecting to RDS using IAM
 authentication.
    /// </summary>
    /// <param name="input">The input event data passed to the Lambda function</
param>
    /// <param name="context">The Lambda execution context that provides runtime
 information</param>
    /// <returns>A response object containing the execution result</returns>

    public async Task<APIGatewayProxyResponse>
 FunctionHandler(APIGatewayProxyRequest request, ILambdaContext context)
    {
        // Sample Input: {"body": "{\"key1\":\"20\", \"key2\":\"25\"}"}
        var input = JsonSerializer.Deserialize<InputModel>(request.Body);

        /// Obtain authentication token
        var authToken = RDSAuthTokenGenerator.GenerateAuthToken(
            Environment.GetEnvironmentVariable("RDS_ENDPOINT"),
            Convert.ToInt32(Environment.GetEnvironmentVariable("RDS_PORT")),
            Environment.GetEnvironmentVariable("RDS_USERNAME")
        );

        /// Build the Connection String with the Token
        string connectionString =
 $"Server={Environment.GetEnvironmentVariable("RDS_ENDPOINT")};" +

 $"Port={Environment.GetEnvironmentVariable("RDS_PORT")};" +
```

```
$"Uid={Environment.GetEnvironmentVariable("RDS_USERNAME")};" +
                                $"Pwd={authToken};";


       try
       {
           await using var connection = new MySqlConnection(connectionString);
           await connection.OpenAsync();

           const string sql = "SELECT @param1 + @param2 AS Sum";

           await using var command = new MySqlCommand(sql, connection);
           command.Parameters.AddWithValue("@param1", int.Parse(input.key1 ??
"0"));
           command.Parameters.AddWithValue("@param2", int.Parse(input.key2 ??
"0"));

           await using var reader = await command.ExecuteReaderAsync();
           if (await reader.ReadAsync())
           {
               int result = reader.GetInt32("Sum");

               //Sample Response: {"statusCode":200,"body":"{\"message\":\"The
sum is: 45\"}","isBase64Encoded":false}
               return new APIGatewayProxyResponse
               {
                   StatusCode = 200,
                   Body = JsonSerializer.Serialize(new { message = $"The sum is:
{result}" })
               };
           }

       }
       catch (Exception ex)
       {
           Console.WriteLine($"Error: {ex.Message}");
       }

       return new APIGatewayProxyResponse
       {
           StatusCode = 500,
           Body = JsonSerializer.Serialize(new { error = "Internal server
error" })
```

```
        };
    }
}
```

Go

Kit SDK pour Go V2

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Connexion à une base de données Amazon RDS dans une fonction Lambda à l'aide de Go.

```
/*
Golang v2 code here.
*/

package main

import (
 "context"
 "database/sql"
 "encoding/json"
 "fmt"
 "os"

 "github.com/aws/aws-lambda-go/lambda"
 "github.com/aws/aws-sdk-go-v2/config"
 "github.com/aws/aws-sdk-go-v2/feature/rds/auth"
 _ "github.com/go-sql-driver/mysql"
)

type MyEvent struct {
 Name string `json:"name"`
}

func HandleRequest(event *MyEvent) (map[string]interface{}, error) {
```

```
var dbName string = os.Getenv("DatabaseName")
var dbUser string = os.Getenv("DatabaseUser")
var dbHost string = os.Getenv("DBHost") // Add hostname without https
var dbPort int = os.Getenv("Port")      // Add port number
var dbEndpoint string = fmt.Sprintf("%s:%d", dbHost, dbPort)
var region string = os.Getenv("AWS_REGION")

cfg, err := config.LoadDefaultConfig(context.TODO())
if err != nil {
 panic("configuration error: " + err.Error())
}

authenticationToken, err := auth.BuildAuthToken(
 context.TODO(), dbEndpoint, region, dbUser, cfg.Credentials)
if err != nil {
 panic("failed to create authentication token: " + err.Error())
}

dsn := fmt.Sprintf("%s:%s@tcp(%s)/%s?tls=true&allowCleartextPasswords=true",
 dbUser, authenticationToken, dbEndpoint, dbName,
)

db, err := sql.Open("mysql", dsn)
if err != nil {
 panic(err)
}

defer db.Close()

var sum int
err = db.QueryRow("SELECT ?+? AS sum", 3, 2).Scan(&sum)
if err != nil {
 panic(err)
}
s := fmt.Sprint(sum)
message := fmt.Sprintf("The selected sum is: %s", s)

messageBytes, err := json.Marshal(message)
if err != nil {
 return nil, err
}

messageString := string(messageBytes)
return map[string]interface{}{
```

```
  "statusCode": 200,
  "headers":    map[string]string{"Content-Type": "application/json"},
  "body":       messageString,
 }, nil
}

func main() {
 lambda.Start(HandleRequest)
}
```

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Connexion à une base de données Amazon RDS dans une fonction Lambda à l'aide de Java.

```
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.APIGatewayProxyRequestEvent;
import com.amazonaws.services.lambda.runtime.events.APIGatewayProxyResponseEvent;
import software.amazon.awssdk.auth.credentials.DefaultCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.rdsdata.RdsDataClient;
import software.amazon.awssdk.services.rdsdata.model.ExecuteStatementRequest;
import software.amazon.awssdk.services.rdsdata.model.ExecuteStatementResponse;
import software.amazon.awssdk.services.rdsdata.model.Field;

import java.sql.Connection;
import java.sql.DriverManager;
import java.sql.PreparedStatement;
import java.sql.ResultSet;

public class RdsLambdaHandler implements
 RequestHandler<APIGatewayProxyRequestEvent, APIGatewayProxyResponseEvent> {
```

```
    @Override
    public APIGatewayProxyResponseEvent handleRequest(APIGatewayProxyRequestEvent
 event, Context context) {
        APIGatewayProxyResponseEvent response = new
 APIGatewayProxyResponseEvent();

        try {
            // Obtain auth token
            String token = createAuthToken();

            // Define connection configuration
            String connectionString = String.format("jdbc:mysql://%s:%s/%s?
useSSL=true&requireSSL=true",
                    System.getenv("ProxyHostName"),
                    System.getenv("Port"),
                    System.getenv("DBName"));

            // Establish a connection to the database
            try (Connection connection =
 DriverManager.getConnection(connectionString, System.getenv("DBUserName"),
 token);
                 PreparedStatement statement =
 connection.prepareStatement("SELECT ? + ? AS sum")) {

                statement.setInt(1, 3);
                statement.setInt(2, 2);

                try (ResultSet resultSet = statement.executeQuery()) {
                    if (resultSet.next()) {
                        int sum = resultSet.getInt("sum");
                        response.setStatusCode(200);
                        response.setBody("The selected sum is: " + sum);
                    }
                }
            }

        } catch (Exception e) {
            response.setStatusCode(500);
            response.setBody("Error: " + e.getMessage());
        }

        return response;
    }
```

```
    private String createAuthToken() {
        // Create RDS Data Service client
        RdsDataClient rdsDataClient = RdsDataClient.builder()
                .region(Region.of(System.getenv("AWS_REGION")))
                .credentialsProvider(DefaultCredentialsProvider.create())
                .build();

        // Define authentication request
        ExecuteStatementRequest request = ExecuteStatementRequest.builder()
                .resourceArn(System.getenv("ProxyHostName"))
                .secretArn(System.getenv("DBUserName"))
                .database(System.getenv("DBName"))
                .sql("SELECT 'RDS IAM Authentication'")
                .build();

        // Execute request and obtain authentication token
        ExecuteStatementResponse response =
 rdsDataClient.executeStatement(request);
        Field tokenField = response.records().get(0).get(0);

        return tokenField.stringValue();
    }
}
```

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Connexion à une base de données Amazon RDS dans une fonction Lambda à l'aide JavaScript.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
/*
```

```
Node.js code here.
*/
// ES6+ example
import { Signer } from "@aws-sdk/rds-signer";
import mysql from 'mysql2/promise';

async function createAuthToken() {
  // Define connection authentication parameters
  const dbinfo = {

    hostname: process.env.ProxyHostName,
    port: process.env.Port,
    username: process.env.DBUserName,
    region: process.env.AWS_REGION,

  }

  // Create RDS Signer object
  const signer = new Signer(dbinfo);

  // Request authorization token from RDS, specifying the username
  const token = await signer.getAuthToken();
  return token;
}

async function dbOps() {

  // Obtain auth token
  const token = await createAuthToken();
  // Define connection configuration
  let connectionConfig = {
    host: process.env.ProxyHostName,
    user: process.env.DBUserName,
    password: token,
    database: process.env.DBName,
    ssl: 'Amazon RDS'
  }
  // Create the connection to the DB
  const conn = await mysql.createConnection(connectionConfig);
  // Obtain the result of the query
  const [res,] = await conn.execute('select ?+? as sum', [3, 2]);
  return res;

}
```

```
export const handler = async (event) => {
  // Execute database flow
  const result = await dbOps();
  // Return result
  return {
    statusCode: 200,
    body: JSON.stringify("The selected sum is: " + result[0].sum)
  }
};
```

Connexion à une base de données Amazon RDS dans une fonction Lambda à l'aide TypeScript.

```
import { Signer } from "@aws-sdk/rds-signer";
import mysql from 'mysql2/promise';

// RDS settings
// Using '!' (non-null assertion operator) to tell the TypeScript compiler that
 the DB settings are not null or undefined,
const proxy_host_name = process.env.PROXY_HOST_NAME!
const port = parseInt(process.env.PORT!)
const db_name = process.env.DB_NAME!
const db_user_name = process.env.DB_USER_NAME!
const aws_region = process.env.AWS_REGION!


async function createAuthToken(): Promise<string> {

    // Create RDS Signer object
    const signer = new Signer({
        hostname: proxy_host_name,
        port: port,
        region: aws_region,
        username: db_user_name
    });

    // Request authorization token from RDS, specifying the username
    const token = await signer.getAuthToken();
    return token;
}
```

```
async function dbOps(): Promise<mysql.QueryResult | undefined> {
    try {
        // Obtain auth token
        const token = await createAuthToken();
        const conn = await mysql.createConnection({
            host: proxy_host_name,
            user: db_user_name,
            password: token,
            database: db_name,
            ssl: 'Amazon RDS' // Ensure you have the CA bundle for SSL connection
        });
        const [rows, fields] = await conn.execute('SELECT ? + ? AS sum', [3, 2]);
        console.log('result:', rows);
        return rows;
    }
    catch (err) {
        console.log(err);
    }
}

export const lambdaHandler = async (event: any): Promise<{ statusCode: number;
 body: string }> => {
    // Execute database flow
    const result = await dbOps();

    // Return error is result is undefined
    if (result == undefined)
        return {
            statusCode: 500,
            body: JSON.stringify(`Error with connection to DB host`)
        }

    // Return result
    return {
        statusCode: 200,
        body: JSON.stringify(`The selected sum is: ${result[0].sum}`)
    };
};
```

PHP

Kit SDK pour PHP

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Connexion à une base de données Amazon RDS dans une fonction Lambda à l'aide de PHP.

```
<?php
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0

# using bref/bref and bref/logger for simplicity

use Bref\Context\Context;
use Bref\Event\Handler as StdHandler;
use Bref\Logger\StderrLogger;
use Aws\Rds\AuthTokenGenerator;
use Aws\Credentials\CredentialProvider;

require __DIR__ . '/vendor/autoload.php';

class Handler implements StdHandler
{
    private StderrLogger $logger;
    public function __construct(StderrLogger $logger)
    {
        $this->logger = $logger;
    }


    private function getAuthToken(): string {
        // Define connection authentication parameters
        $dbConnection = [
            'hostname' => getenv('DB_HOSTNAME'),
            'port' => getenv('DB_PORT'),
            'username' => getenv('DB_USERNAME'),
            'region' => getenv('AWS_REGION'),
        ];
```

```
        // Create RDS AuthTokenGenerator object
        $generator = new
AuthTokenGenerator(CredentialProvider::defaultProvider());

        // Request authorization token from RDS, specifying the username
        return $generator->createToken(
            $dbConnection['hostname'] . ':' . $dbConnection['port'],
            $dbConnection['region'],
            $dbConnection['username']
        );
    }

    private function getQueryResults() {
        // Obtain auth token
        $token = $this->getAuthToken();

        // Define connection configuration
        $connectionConfig = [
            'host' => getenv('DB_HOSTNAME'),
            'user' => getenv('DB_USERNAME'),
            'password' => $token,
            'database' => getenv('DB_NAME'),
        ];

        // Create the connection to the DB
        $conn = new PDO(

"mysql:host={$connectionConfig['host']};dbname={$connectionConfig['database']}",
            $connectionConfig['user'],
            $connectionConfig['password'],
            [
                PDO::MYSQL_ATTR_SSL_CA => '/path/to/rds-ca-2019-root.pem',
                PDO::MYSQL_ATTR_SSL_VERIFY_SERVER_CERT => true,
            ]
        );

        // Obtain the result of the query
        $stmt = $conn->prepare('SELECT ?+? AS sum');
        $stmt->execute([3, 2]);

        return $stmt->fetch(PDO::FETCH_ASSOC);
    }
```

```
    /**
     * @param mixed $event
     * @param Context $context
     * @return array
     */
    public function handle(mixed $event, Context $context): array
    {
        $this->logger->info("Processing query");

        // Execute database flow
        $result = $this->getQueryResults();

        return [
            'sum' => $result['sum']
        ];
    }
}

$logger = new StderrLogger();
return new Handler($logger);
```

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Connexion à une base de données Amazon RDS dans une fonction Lambda à l'aide de Python.

```
import json
import os
import boto3
import pymysql

# RDS settings
proxy_host_name = os.environ['PROXY_HOST_NAME']
```

```
port = int(os.environ['PORT'])
db_name = os.environ['DB_NAME']
db_user_name = os.environ['DB_USER_NAME']
aws_region = os.environ['AWS_REGION']


# Fetch RDS Auth Token
def get_auth_token():
    client = boto3.client('rds')
    token = client.generate_db_auth_token(
        DBHostname=proxy_host_name,
        Port=port
        DBUsername=db_user_name
        Region=aws_region
    )
    return token

def lambda_handler(event, context):
    token = get_auth_token()
    try:
        connection = pymysql.connect(
            host=proxy_host_name,
            user=db_user_name,
            password=token,
            db=db_name,
            port=port,
            ssl={'ca': 'Amazon RDS'}  # Ensure you have the CA bundle for SSL
 connection
        )

        with connection.cursor() as cursor:
            cursor.execute('SELECT %s + %s AS sum', (3, 2))
            result = cursor.fetchone()

        return result

    except Exception as e:
        return (f"Error: {str(e)}")  # Return an error message if an exception
 occurs
```

Ruby

Kit SDK pour Ruby

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Connexion à une base de données Amazon RDS dans une fonction Lambda à l'aide de Ruby.

```
# Ruby code here.

require 'aws-sdk-rds'
require 'json'
require 'mysql2'

def lambda_handler(event:, context:)
  endpoint = ENV['DBEndpoint'] # Add the endpoint without https"
  port = ENV['Port']           # 3306
  user = ENV['DBUser']
  region = ENV['DBRegion']     # 'us-east-1'
  db_name = ENV['DBName']

  credentials = Aws::Credentials.new(
    ENV['AWS_ACCESS_KEY_ID'],
    ENV['AWS_SECRET_ACCESS_KEY'],
    ENV['AWS_SESSION_TOKEN']
  )
  rds_client = Aws::RDS::AuthTokenGenerator.new(
    region: region,
    credentials: credentials
  )

  token = rds_client.auth_token(
    endpoint: endpoint+ ':' + port,
    user_name: user,
    region: region
  )

  begin
    conn = Mysql2::Client.new(
```

```
      host: endpoint,
      username: user,
      password: token,
      port: port,
      database: db_name,
      sslca: '/var/task/global-bundle.pem',
      sslverify: true,
      enable_cleartext_plugin: true
    )
    a = 3
    b = 2
    result = conn.query("SELECT #{a} + #{b} AS sum").first['sum']
    puts result
    conn.close
    {
      statusCode: 200,
      body: result.to_json
    }
  rescue => e
    puts "Database connection failed due to #{e}"
  end
end
```

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Connexion à une base de données Amazon RDS dans une fonction Lambda à l'aide de Rust.

```
use aws_config::BehaviorVersion;
use aws_credential_types::provider::ProvideCredentials;
use aws_sigv4::{
    http_request::{sign, SignableBody, SignableRequest, SigningSettings},
    sign::v4,
};
use lambda_runtime::{run, service_fn, Error, LambdaEvent};
```

```
use serde_json::{json, Value};
use sqlx::postgres::PgConnectOptions;
use std::env;
use std::time::{Duration, SystemTime};

const RDS_CERTS: &[u8] = include_bytes!("global-bundle.pem");

async fn generate_rds_iam_token(
    db_hostname: &str,
    port: u16,
    db_username: &str,
) -> Result<String, Error> {
    let config = aws_config::load_defaults(BehaviorVersion::v2024_03_28()).await;

    let credentials = config
        .credentials_provider()
        .expect("no credentials provider found")
        .provide_credentials()
        .await
        .expect("unable to load credentials");
    let identity = credentials.into();
    let region = config.region().unwrap().to_string();

    let mut signing_settings = SigningSettings::default();
    signing_settings.expires_in = Some(Duration::from_secs(900));
    signing_settings.signature_location =
 aws_sigv4::http_request::SignatureLocation::QueryParams;

    let signing_params = v4::SigningParams::builder()
        .identity(&identity)
        .region(&region)
        .name("rds-db")
        .time(SystemTime::now())
        .settings(signing_settings)
        .build()?;

    let url = format!(
        "https://{db_hostname}:{port}/?Action=connect&DBUser={db_user}",
        db_hostname = db_hostname,
        port = port,
        db_user = db_username
    );

    let signable_request =
```

```
        SignableRequest::new("GET", &url, std::iter::empty(),
 SignableBody::Bytes(&[]))
            .expect("signable request");

    let (signing_instructions, _signature) =
        sign(signable_request, &signing_params.into())?.into_parts();

    let mut url = url::Url::parse(&url).unwrap();
    for (name, value) in signing_instructions.params() {
        url.query_pairs_mut().append_pair(name, &value);
    }

    let response = url.to_string().split_off("https://".len());

    Ok(response)
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    run(service_fn(handler)).await
}

async fn handler(_event: LambdaEvent<Value>) -> Result<Value, Error> {
    let db_host = env::var("DB_HOSTNAME").expect("DB_HOSTNAME must be set");
    let db_port = env::var("DB_PORT")
        .expect("DB_PORT must be set")
        .parse::<u16>()
        .expect("PORT must be a valid number");
    let db_name = env::var("DB_NAME").expect("DB_NAME must be set");
    let db_user_name = env::var("DB_USERNAME").expect("DB_USERNAME must be set");

    let token = generate_rds_iam_token(&db_host, db_port, &db_user_name).await?;

    let opts = PgConnectOptions::new()
        .host(&db_host)
        .port(db_port)
        .username(&db_user_name)
        .password(&token)
        .database(&db_name)
        .ssl_root_cert_from_pem(RDS_CERTS.to_vec())
        .ssl_mode(sqlx::postgres::PgSslMode::Require);

    let pool = sqlx::postgres::PgPoolOptions::new()
        .connect_with(opts)
```

```
        .await?;

    let result: i32 = sqlx::query_scalar("SELECT $1 + $2")
        .bind(3)
        .bind(2)
        .fetch_one(&pool)
        .await?;

    println!("Result: {:?}", result);

    Ok(json!({
        "statusCode": 200,
        "content-type": "text/plain",
        "body": format!("The selected sum is: {result}")
    }))
}
```

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Invoquer une fonction Lambda à partir d'un déclencheur Kinesis

Les exemples de code suivants montrent comment implémenter une fonction Lambda qui reçoit un événement déclenché par la réception d'enregistrements à partir d'un flux Kinesis. La fonction récupère la charge utile Kinesis, décode à partir de Base64 et enregistre le contenu de l'enregistrement.

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement Kinesis avec Lambda à l'aide de .NET.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
using System.Text;
using Amazon.Lambda.Core;
using Amazon.Lambda.KinesisEvents;
using AWS.Lambda.Powertools.Logging;

// Assembly attribute to enable the Lambda function's JSON input to be converted
 into a .NET class.
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSeri

namespace KinesisIntegrationSampleCode;

public class Function
{
    // Powertools Logger requires an environment variables against your function
    // POWERTOOLS_SERVICE_NAME
    [Logging(LogEvent = true)]
    public async Task FunctionHandler(KinesisEvent evnt, ILambdaContext context)
    {
        if (evnt.Records.Count == 0)
        {
            Logger.LogInformation("Empty Kinesis Event received");
            return;
        }

        foreach (var record in evnt.Records)
        {
            try
            {
                Logger.LogInformation($"Processed Event with EventId:
 {record.EventId}");
                string data = await GetRecordDataAsync(record.Kinesis, context);
                Logger.LogInformation($"Data: {data}");
                // TODO: Do interesting work based on the new data
            }
            catch (Exception ex)
            {
                Logger.LogError($"An error occurred {ex.Message}");
                throw;
            }
        }
```

```
        Logger.LogInformation($"Successfully processed {evnt.Records.Count}
 records.");
    }

    private async Task<string> GetRecordDataAsync(KinesisEvent.Record record,
 ILambdaContext context)
    {
        byte[] bytes = record.Data.ToArray();
        string data = Encoding.UTF8.GetString(bytes);
        await Task.CompletedTask; //Placeholder for actual async work
        return data;
    }
}
```

Go

Kit SDK pour Go V2

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement Kinesis avec Lambda à l'aide de Go.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package main

import (
 "context"
 "log"

 "github.com/aws/aws-lambda-go/events"
 "github.com/aws/aws-lambda-go/lambda"
)

func handler(ctx context.Context, kinesisEvent events.KinesisEvent) error {
 if len(kinesisEvent.Records) == 0 {
  log.Printf("empty Kinesis event received")
  return nil
```

```
 }

 for _, record := range kinesisEvent.Records {
  log.Printf("processed Kinesis event with EventId: %v", record.EventID)
  recordDataBytes := record.Kinesis.Data
  recordDataText := string(recordDataBytes)
  log.Printf("record data: %v", recordDataText)
  // TODO: Do interesting work based on the new data
 }
 log.Printf("successfully processed %v records", len(kinesisEvent.Records))
 return nil
}

func main() {
 lambda.Start(handler)
}
```

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement Kinesis avec Lambda à l'aide de Java.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package example;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.LambdaLogger;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.KinesisEvent;

public class Handler implements RequestHandler<KinesisEvent, Void> {
    @Override
    public Void handleRequest(final KinesisEvent event, final Context context) {
```

```
        LambdaLogger logger = context.getLogger();
        if (event.getRecords().isEmpty()) {
            logger.log("Empty Kinesis Event received");
            return null;
        }
        for (KinesisEvent.KinesisEventRecord record : event.getRecords()) {
            try {
                logger.log("Processed Event with EventId: "+record.getEventID());
                String data = new String(record.getKinesis().getData().array());
                logger.log("Data:"+ data);
                // TODO: Do interesting work based on the new data
            }
            catch (Exception ex) {
                logger.log("An error occurred:"+ex.getMessage());
                throw ex;
            }
        }
        logger.log("Successfully processed:"+event.getRecords().size()+"
 records");
        return null;
    }

}
```

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement Kinesis avec Lambda à l'aide de JavaScript.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
exports.handler = async (event, context) => {
  for (const record of event.Records) {
    try {
```

```
      console.log(`Processed Kinesis Event - EventID: ${record.eventID}`);
      const recordData = await getRecordDataAsync(record.kinesis);
      console.log(`Record Data: ${recordData}`);
      // TODO: Do interesting work based on the new data
    } catch (err) {
      console.error(`An error occurred ${err}`);
      throw err;
    }
  }
  console.log(`Successfully processed ${event.Records.length} records.`);
};

async function getRecordDataAsync(payload) {
  var data = Buffer.from(payload.data, "base64").toString("utf-8");
  await Promise.resolve(1); //Placeholder for actual async work
  return data;
}
```

Consommation d'un événement Kinesis avec Lambda à l'aide de TypeScript.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import {
  KinesisStreamEvent,
  Context,
  KinesisStreamHandler,
  KinesisStreamRecordPayload,
} from "aws-lambda";
import { Buffer } from "buffer";
import { Logger } from "@aws-lambda-powertools/logger";

const logger = new Logger({
  logLevel: "INFO",
  serviceName: "kinesis-stream-handler-sample",
});

export const functionHandler: KinesisStreamHandler = async (
  event: KinesisStreamEvent,
  context: Context
): Promise<void> => {
  for (const record of event.Records) {
    try {
```

```
      logger.info(`Processed Kinesis Event - EventID: ${record.eventID}`);
      const recordData = await getRecordDataAsync(record.kinesis);
      logger.info(`Record Data: ${recordData}`);
      // TODO: Do interesting work based on the new data
    } catch (err) {
      logger.error(`An error occurred ${err}`);
      throw err;
    }
    logger.info(`Successfully processed ${event.Records.length} records.`);
  }
};

async function getRecordDataAsync(
  payload: KinesisStreamRecordPayload
): Promise<string> {
  var data = Buffer.from(payload.data, "base64").toString("utf-8");
  await Promise.resolve(1); //Placeholder for actual async work
  return data;
}
```

PHP

Kit SDK pour PHP

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement Kinesis avec Lambda à l'aide de PHP.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
<?php

# using bref/bref and bref/logger for simplicity

use Bref\Context\Context;
use Bref\Event\Kinesis\KinesisEvent;
use Bref\Event\Kinesis\KinesisHandler;
```

```
use Bref\Logger\StderrLogger;

require __DIR__ . '/vendor/autoload.php';

class Handler extends KinesisHandler
{
    private StderrLogger $logger;
    public function __construct(StderrLogger $logger)
    {
        $this->logger = $logger;
    }

    /**
     * @throws JsonException
     * @throws \Bref\Event\InvalidLambdaEvent
     */
    public function handleKinesis(KinesisEvent $event, Context $context): void
    {
        $this->logger->info("Processing records");
        $records = $event->getRecords();
        foreach ($records as $record) {
            $data = $record->getData();
            $this->logger->info(json_encode($data));
            // TODO: Do interesting work based on the new data

            // Any exception thrown will be logged and the invocation will be
 marked as failed
        }
        $totalRecords = count($records);
        $this->logger->info("Successfully processed $totalRecords records");
    }
}

$logger = new StderrLogger();
return new Handler($logger);
```

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement Kinesis avec Lambda à l'aide de Python.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
import base64
def lambda_handler(event, context):

    for record in event['Records']:
        try:
            print(f"Processed Kinesis Event - EventID: {record['eventID']}")
            record_data = base64.b64decode(record['kinesis']
['data']).decode('utf-8')
            print(f"Record Data: {record_data}")
            # TODO: Do interesting work based on the new data
        except Exception as e:
            print(f"An error occurred {e}")
            raise e
    print(f"Successfully processed {len(event['Records'])} records.")
```

Ruby

Kit SDK pour Ruby

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement Kinesis avec Lambda à l'aide de Ruby.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
require 'aws-sdk'

def lambda_handler(event:, context:)
  event['Records'].each do |record|
    begin
      puts "Processed Kinesis Event - EventID: #{record['eventID']}"
      record_data = get_record_data_async(record['kinesis'])
      puts "Record Data: #{record_data}"
      # TODO: Do interesting work based on the new data
    rescue => err
      $stderr.puts "An error occurred #{err}"
      raise err
    end
  end
  puts "Successfully processed #{event['Records'].length} records."
end

def get_record_data_async(payload)
  data = Base64.decode64(payload['data']).force_encoding('UTF-8')
  # Placeholder for actual async work
  # You can use Ruby's asynchronous programming tools like async/await or fibers
 here.
  return data
end
```

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement Kinesis avec Lambda à l'aide de Rust.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
use aws_lambda_events::event::kinesis::KinesisEvent;
use lambda_runtime::{run, service_fn, Error, LambdaEvent};

async fn function_handler(event: LambdaEvent<KinesisEvent>) -> Result<(), Error>
 {
    if event.payload.records.is_empty() {
        tracing::info!("No records found. Exiting.");
        return Ok(());
    }

    event.payload.records.iter().for_each(|record| {
        tracing::info!("EventId:
 {}",record.event_id.as_deref().unwrap_or_default());

        let record_data = std::str::from_utf8(&record.kinesis.data);

        match record_data {
            Ok(data) => {
                // log the record data
                tracing::info!("Data: {}", data);
            }
            Err(e) => {
                tracing::error!("Error: {}", e);
            }
        }
    });

    tracing::info!(
        "Successfully processed {} records",
        event.payload.records.len()
    );

    Ok(())
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    tracing_subscriber::fmt()
        .with_max_level(tracing::Level::INFO)
        // disable printing the name of the module in every log line.
        .with_target(false)
```

```
        // disabling time is handy because CloudWatch will add the ingestion
 time.
        .without_time()
        .init();

    run(service_fn(function_handler)).await
}
```

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Invocation d'une fonction Lambda à partir d'un déclencheur DynamoDB

Les exemples de code suivants illustrent comment implémenter une fonction Lambda qui reçoit un événement déclenché par la réception d'enregistrements à partir d'un flux DynamoDB. La fonction récupère les données utiles DynamoDB et journalise le contenu de l'enregistrement.

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement DynamoDB avec Lambda en utilisant .NET.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
using System.Text.Json;
using System.Text;
using Amazon.Lambda.Core;
using Amazon.Lambda.DynamoDBEvents;

// Assembly attribute to enable the Lambda function's JSON input to be converted
 into a .NET class.
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSeri
```

```
namespace AWSLambda_DDB;

public class Function
{
    public void FunctionHandler(DynamoDBEvent dynamoEvent, ILambdaContext
 context)
    {
        context.Logger.LogInformation($"Beginning to process
 {dynamoEvent.Records.Count} records...");

        foreach (var record in dynamoEvent.Records)
        {
            context.Logger.LogInformation($"Event ID: {record.EventID}");
            context.Logger.LogInformation($"Event Name: {record.EventName}");

            context.Logger.LogInformation(JsonSerializer.Serialize(record));
        }

        context.Logger.LogInformation("Stream processing complete.");
    }
}
```

Go

Kit SDK pour Go V2

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement DynamoDB avec Lambda en utilisant Go.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package main

import (
 "context"
```

```
 "github.com/aws/aws-lambda-go/lambda"
 "github.com/aws/aws-lambda-go/events"
 "fmt"
)

func HandleRequest(ctx context.Context, event events.DynamoDBEvent) (*string,
 error) {
 if len(event.Records) == 0 {
  return nil, fmt.Errorf("received empty event")
 }

 for _, record := range event.Records {
   LogDynamoDBRecord(record)
 }

 message := fmt.Sprintf("Records processed: %d", len(event.Records))
 return &message, nil
}

func main() {
 lambda.Start(HandleRequest)
}

func LogDynamoDBRecord(record events.DynamoDBEventRecord){
 fmt.Println(record.EventID)
 fmt.Println(record.EventName)
 fmt.Printf("%+v\n", record.Change)
}
```

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement DynamoDB avec Lambda en utilisant Java.

```
import com.amazonaws.services.lambda.runtime.Context;
```

```
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.DynamodbEvent;
import
 com.amazonaws.services.lambda.runtime.events.DynamodbEvent.DynamodbStreamRecord;
import com.google.gson.Gson;
import com.google.gson.GsonBuilder;

public class example implements RequestHandler<DynamodbEvent, Void> {

    private static final Gson GSON = new
 GsonBuilder().setPrettyPrinting().create();

    @Override
    public Void handleRequest(DynamodbEvent event, Context context) {
        System.out.println(GSON.toJson(event));
        event.getRecords().forEach(this::logDynamoDBRecord);
        return null;
    }

    private void logDynamoDBRecord(DynamodbStreamRecord record) {
        System.out.println(record.getEventID());
        System.out.println(record.getEventName());
        System.out.println("DynamoDB Record: " +
 GSON.toJson(record.getDynamodb()));
    }
}
```

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement DynamoDB avec Lambda à l'aide de JavaScript.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
exports.handler = async (event, context) => {
```

```
    console.log(JSON.stringify(event, null, 2));
    event.Records.forEach(record => {
        logDynamoDBRecord(record);
    });
};

const logDynamoDBRecord = (record) => {
    console.log(record.eventID);
    console.log(record.eventName);
    console.log(`DynamoDB Record: ${JSON.stringify(record.dynamodb)}`);
};
```

Consommation d'un événement DynamoDB avec Lambda à l'aide de TypeScript.

```
export const handler = async (event, context) => {
    console.log(JSON.stringify(event, null, 2));
    event.Records.forEach(record => {
        logDynamoDBRecord(record);
    });
}
const logDynamoDBRecord = (record) => {
    console.log(record.eventID);
    console.log(record.eventName);
    console.log(`DynamoDB Record: ${JSON.stringify(record.dynamodb)}`);
};
```

PHP

Kit SDK pour PHP

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l’exemple complet et découvrez comment le configurer et l’exécuter dans le référentiel d’exemples sans serveur.

Consommation d’un événement DynamoDB avec Lambda en utilisant PHP.

```
<?php
```

```
# using bref/bref and bref/logger for simplicity

use Bref\Context\Context;
use Bref\Event\DynamoDb\DynamoDbEvent;
use Bref\Event\DynamoDb\DynamoDbHandler;
use Bref\Logger\StderrLogger;

require __DIR__ . '/vendor/autoload.php';

class Handler extends DynamoDbHandler
{
    private StderrLogger $logger;

    public function __construct(StderrLogger $logger)
    {
        $this->logger = $logger;
    }

    /**
     * @throws JsonException
     * @throws \Bref\Event\InvalidLambdaEvent
     */
    public function handleDynamoDb(DynamoDbEvent $event, Context $context): void
    {
        $this->logger->info("Processing DynamoDb table items");
        $records = $event->getRecords();

        foreach ($records as $record) {
            $eventName = $record->getEventName();
            $keys = $record->getKeys();
            $old = $record->getOldImage();
            $new = $record->getNewImage();

            $this->logger->info("Event Name:".$eventName."\n");
            $this->logger->info("Keys:". json_encode($keys)."\n");
            $this->logger->info("Old Image:". json_encode($old)."\n");
            $this->logger->info("New Image:". json_encode($new));

            // TODO: Do interesting work based on the new data

            // Any exception thrown will be logged and the invocation will be
 marked as failed
        }
```

```
        $totalRecords = count($records);
        $this->logger->info("Successfully processed $totalRecords items");
    }
}

$logger = new StderrLogger();
return new Handler($logger);
```

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement DynamoDB avec Lambda en utilisant Python.

```
import json

def lambda_handler(event, context):
    print(json.dumps(event, indent=2))

    for record in event['Records']:
        log_dynamodb_record(record)

def log_dynamodb_record(record):
    print(record['eventID'])
    print(record['eventName'])
    print(f"DynamoDB Record: {json.dumps(record['dynamodb'])}")
```

Ruby

Kit SDK pour Ruby

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement DynamoDB avec Lambda en utilisant Ruby.

```
def lambda_handler(event:, context:)
    return 'received empty event' if event['Records'].empty?

    event['Records'].each do |record|
      log_dynamodb_record(record)
    end

    "Records processed: #{event['Records'].length}"
  end

  def log_dynamodb_record(record)
    puts record['eventID']
    puts record['eventName']
    puts "DynamoDB Record: #{JSON.generate(record['dynamodb'])}"
  end
```

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement DynamoDB avec Lambda en utilisant Rust.

```
use lambda_runtime::{service_fn, tracing, Error, LambdaEvent};
use aws_lambda_events::{
    event::dynamodb::{Event, EventRecord},
   };


// Built with the following dependencies:
//lambda_runtime = "0.11.1"
//serde_json = "1.0"
//tokio = { version = "1", features = ["macros"] }
//tracing = { version = "0.1", features = ["log"] }
//tracing-subscriber = { version = "0.3", default-features = false, features =
 ["fmt"] }
//aws_lambda_events = "0.15.0"

async fn function_handler(event: LambdaEvent<Event>) ->Result<(), Error> {

    let records = &event.payload.records;
    tracing::info!("event payload: {:?}",records);
    if records.is_empty() {
        tracing::info!("No records found. Exiting.");
        return Ok(());
    }

    for record in records{
        log_dynamo_dbrecord(record);
    }

    tracing::info!("Dynamo db records processed");

    // Prepare the response
    Ok(())

}

fn log_dynamo_dbrecord(record: &EventRecord)-> Result<(), Error>{
    tracing::info!("EventId: {}", record.event_id);
    tracing::info!("EventName: {}", record.event_name);
    tracing::info!("DynamoDB Record: {:?}", record.change );
    Ok(())
```

```
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    tracing_subscriber::fmt()
    .with_max_level(tracing::Level::INFO)
    .with_target(false)
    .without_time()
    .init();

    let func = service_fn(function_handler);
    lambda_runtime::run(func).await?;
    Ok(())

}
```

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Invocation d'une fonction Lambda à partir d'un déclencheur Amazon DocumentDB

Les exemples de code suivants illustrent comment implémenter une fonction Lambda qui reçoit un événement déclenché par la réception d'enregistrements à partir d'un flux de modification DocumentDB. La fonction récupère les données utiles DocumentDB et journalise le contenu de l'enregistrement.

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement Amazon DocumentDB avec Lambda en utilisant .NET.

```
using Amazon.Lambda.Core;
using System.Text.Json;
using System;
using System.Collections.Generic;
using System.Text.Json.Serialization;
//Assembly attribute to enable the Lambda function's JSON input to be converted
 into a .NET class.
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSeri

namespace LambdaDocDb;

public class Function
{

     /// <summary>
    /// Lambda function entry point to process Amazon DocumentDB events.
    /// </summary>
    /// <param name="event">The Amazon DocumentDB event.</param>
    /// <param name="context">The Lambda context object.</param>
    /// <returns>A string to indicate successful processing.</returns>
    public string FunctionHandler(Event evnt, ILambdaContext context)
    {

        foreach (var record in evnt.Events)
        {
            ProcessDocumentDBEvent(record, context);
        }

        return "OK";
    }

     private void ProcessDocumentDBEvent(DocumentDBEventRecord record,
 ILambdaContext context)
    {

        var eventData = record.Event;
        var operationType = eventData.OperationType;
        var databaseName = eventData.Ns.Db;
        var collectionName = eventData.Ns.Coll;
        var fullDocument = JsonSerializer.Serialize(eventData.FullDocument, new
 JsonSerializerOptions { WriteIndented = true });
```

```
        context.Logger.LogLine($"Operation type: {operationType}");
        context.Logger.LogLine($"Database: {databaseName}");
        context.Logger.LogLine($"Collection: {collectionName}");
        context.Logger.LogLine($"Full document:\n{fullDocument}");
    }



    public class Event
    {
        [JsonPropertyName("eventSourceArn")]
        public string EventSourceArn { get; set; }

        [JsonPropertyName("events")]
        public List<DocumentDBEventRecord> Events { get; set; }

        [JsonPropertyName("eventSource")]
        public string EventSource { get; set; }
    }

    public class DocumentDBEventRecord
    {
        [JsonPropertyName("event")]
        public EventData Event { get; set; }
    }

    public class EventData
    {
        [JsonPropertyName("_id")]
        public IdData Id { get; set; }

        [JsonPropertyName("clusterTime")]
        public ClusterTime ClusterTime { get; set; }

        [JsonPropertyName("documentKey")]
        public DocumentKey DocumentKey { get; set; }

        [JsonPropertyName("fullDocument")]
        public Dictionary<string, object> FullDocument { get; set; }

        [JsonPropertyName("ns")]
        public Namespace Ns { get; set; }

        [JsonPropertyName("operationType")]
```

```
        public string OperationType { get; set; }
    }

    public class IdData
    {
        [JsonPropertyName("_data")]
        public string Data { get; set; }
    }

    public class ClusterTime
    {
        [JsonPropertyName("$timestamp")]
        public Timestamp Timestamp { get; set; }
    }

    public class Timestamp
    {
        [JsonPropertyName("t")]
        public long T { get; set; }

        [JsonPropertyName("i")]
        public int I { get; set; }
    }

    public class DocumentKey
    {
        [JsonPropertyName("_id")]
        public Id Id { get; set; }
    }

    public class Id
    {
        [JsonPropertyName("$oid")]
        public string Oid { get; set; }
    }

    public class Namespace
    {
        [JsonPropertyName("db")]
        public string Db { get; set; }

        [JsonPropertyName("coll")]
        public string Coll { get; set; }
    }
```

```
}
```

Go

Kit SDK pour Go V2

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement Amazon DocumentDB avec Lambda en utilisant Go.

```
package main

import (
 "context"
 "encoding/json"
 "fmt"

 "github.com/aws/aws-lambda-go/lambda"
)

type Event struct {
 Events []Record `json:"events"`
}

type Record struct {
 Event struct {
  OperationType string `json:"operationType"`
  NS            struct {
   DB   string `json:"db"`
   Coll string `json:"coll"`
  } `json:"ns"`
  FullDocument interface{} `json:"fullDocument"`
 } `json:"event"`
}

func main() {
```

```
 lambda.Start(handler)
}

func handler(ctx context.Context, event Event) (string, error) {
 fmt.Println("Loading function")
 for _, record := range event.Events {
  logDocumentDBEvent(record)
 }

 return "OK", nil
}

func logDocumentDBEvent(record Record) {
 fmt.Printf("Operation type: %s\n", record.Event.OperationType)
 fmt.Printf("db: %s\n", record.Event.NS.DB)
 fmt.Printf("collection: %s\n", record.Event.NS.Coll)
 docBytes, _ := json.MarshalIndent(record.Event.FullDocument, "", "  ")
 fmt.Printf("Full document: %s\n", string(docBytes))
}
```

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement Amazon DocumentDB avec Lambda en utilisant Java.

```
import java.util.List;
import java.util.Map;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;

public class Example implements RequestHandler<Map<String, Object>, String> {

    @SuppressWarnings("unchecked")
```

```
    @Override
    public String handleRequest(Map<String, Object> event, Context context) {
        List<Map<String, Object>> events = (List<Map<String, Object>>)
 event.get("events");
        for (Map<String, Object> record : events) {
            Map<String, Object> eventData = (Map<String, Object>)
 record.get("event");
            processEventData(eventData);
        }

        return "OK";
    }

    @SuppressWarnings("unchecked")
    private void processEventData(Map<String, Object> eventData) {
        String operationType = (String) eventData.get("operationType");
        System.out.println("operationType: %s".formatted(operationType));

        Map<String, Object> ns = (Map<String, Object>) eventData.get("ns");

        String db = (String) ns.get("db");
        System.out.println("db: %s".formatted(db));
        String coll = (String) ns.get("coll");
        System.out.println("coll: %s".formatted(coll));

        Map<String, Object> fullDocument = (Map<String, Object>)
 eventData.get("fullDocument");
        System.out.println("fullDocument: %s".formatted(fullDocument));
    }

}
```

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement Amazon DocumentDB avec Lambda à l'aide de JavaScript.

```
console.log('Loading function');
exports.handler = async (event, context) => {
    event.events.forEach(record => {
        logDocumentDBEvent(record);
    });
    return 'OK';
};

const logDocumentDBEvent = (record) => {
    console.log('Operation type: ' + record.event.operationType);
    console.log('db: ' + record.event.ns.db);
    console.log('collection: ' + record.event.ns.coll);
    console.log('Full document:', JSON.stringify(record.event.fullDocument, null,
 2));
};
```

Consommation d'un événement Amazon DocumentDB avec Lambda à l'aide de TypeScript

```
import { DocumentDBEventRecord, DocumentDBEventSubscriptionContext } from 'aws-
lambda';

console.log('Loading function');

export const handler = async (
  event: DocumentDBEventSubscriptionContext,
  context: any
): Promise<string> => {
  event.events.forEach((record: DocumentDBEventRecord) => {
    logDocumentDBEvent(record);
  });
  return 'OK';
};

const logDocumentDBEvent = (record: DocumentDBEventRecord): void => {
  console.log('Operation type: ' + record.event.operationType);
  console.log('db: ' + record.event.ns.db);
  console.log('collection: ' + record.event.ns.coll);
  console.log('Full document:', JSON.stringify(record.event.fullDocument, null,
 2));
```

```
};
```

PHP

Kit SDK pour PHP

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement Amazon DocumentDB avec Lambda en utilisant PHP.

```
<?php

require __DIR__.'/vendor/autoload.php';

use Bref\Context\Context;
use Bref\Event\Handler;

class DocumentDBEventHandler implements Handler
{
    public function handle($event, Context $context): string
    {

        $events = $event['events'] ?? [];
        foreach ($events as $record) {
            $this->logDocumentDBEvent($record['event']);
        }
        return 'OK';
    }

    private function logDocumentDBEvent($event): void
    {
        // Extract information from the event record

        $operationType = $event['operationType'] ?? 'Unknown';
        $db = $event['ns']['db'] ?? 'Unknown';
        $collection = $event['ns']['coll'] ?? 'Unknown';
        $fullDocument = $event['fullDocument'] ?? [];
```

```
        // Log the event details

        echo "Operation type: $operationType\n";
        echo "Database: $db\n";
        echo "Collection: $collection\n";
        echo "Full document: " . json_encode($fullDocument, JSON_PRETTY_PRINT) .
 "\n";
    }
}
return new DocumentDBEventHandler();
```

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement Amazon DocumentDB avec Lambda en utilisant Python.

```
import json

def lambda_handler(event, context):
    for record in event.get('events', []):
        log_document_db_event(record)
    return 'OK'

def log_document_db_event(record):
    event_data = record.get('event', {})
    operation_type = event_data.get('operationType', 'Unknown')
    db = event_data.get('ns', {}).get('db', 'Unknown')
    collection = event_data.get('ns', {}).get('coll', 'Unknown')
    full_document = event_data.get('fullDocument', {})

    print(f"Operation type: {operation_type}")
    print(f"db: {db}")
    print(f"collection: {collection}")
```

```
    print("Full document:", json.dumps(full_document, indent=2))
```

Ruby

Kit SDK pour Ruby

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement Amazon DocumentDB avec Lambda en utilisant Ruby.

```
require 'json'

def lambda_handler(event:, context:)
  event['events'].each do |record|
    log_document_db_event(record)
  end
  'OK'
end

def log_document_db_event(record)
  event_data = record['event'] || {}
  operation_type = event_data['operationType'] || 'Unknown'
  db = event_data.dig('ns', 'db') || 'Unknown'
  collection = event_data.dig('ns', 'coll') || 'Unknown'
  full_document = event_data['fullDocument'] || {}

  puts "Operation type: #{operation_type}"
  puts "db: #{db}"
  puts "collection: #{collection}"
  puts "Full document: #{JSON.pretty_generate(full_document)}"
end
```

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement Amazon DocumentDB avec Lambda en utilisant Rust.

```
use lambda_runtime::{service_fn, tracing, Error, LambdaEvent};
use aws_lambda_events::{
    event::documentdb::{DocumentDbEvent, DocumentDbInnerEvent},
   };


// Built with the following dependencies:
//lambda_runtime = "0.11.1"
//serde_json = "1.0"
//tokio = { version = "1", features = ["macros"] }
//tracing = { version = "0.1", features = ["log"] }
//tracing-subscriber = { version = "0.3", default-features = false, features =
 ["fmt"] }
//aws_lambda_events = "0.15.0"

async fn function_handler(event: LambdaEvent<DocumentDbEvent>) ->Result<(),
 Error> {

    tracing::info!("Event Source ARN: {:?}", event.payload.event_source_arn);
    tracing::info!("Event Source: {:?}", event.payload.event_source);

    let records = &event.payload.events;

    if records.is_empty() {
        tracing::info!("No records found. Exiting.");
        return Ok(());
    }

    for record in records{
        log_document_db_event(record);
```

```
    }

    tracing::info!("Document db records processed");

    // Prepare the response
    Ok(())

}

fn log_document_db_event(record: &DocumentDbInnerEvent)-> Result<(), Error>{
    tracing::info!("Change Event: {:?}", record.event);

    Ok(())

}

#[tokio::main]
async fn main() -> Result<(), Error> {
    tracing_subscriber::fmt()
    .with_max_level(tracing::Level::INFO)
    .with_target(false)
    .without_time()
    .init();

    let func = service_fn(function_handler);
    lambda_runtime::run(func).await?;
    Ok(())

}
```

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Invocation d'une fonction Lambda à partir d'un déclencheur Amazon MSK

Les exemples de code suivants illustrent comment implémenter une fonction Lambda qui reçoit un événement déclenché par la réception d'enregistrements à partir d'un cluster Amazon MSK. La fonction récupère les données utiles MSK et journalise le contenu de l'enregistrement.

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement Amazon MSK avec Lambda en utilisant .NET.

```
using System.Text;
using Amazon.Lambda.Core;
using Amazon.Lambda.KafkaEvents;


// Assembly attribute to enable the Lambda function's JSON input to be converted
 into a .NET class.
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSeri

namespace MSKLambda;

public class Function
{


    /// <param name="input">The event for the Lambda function handler to
 process.</param>
    /// <param name="context">The ILambdaContext that provides methods for
 logging and describing the Lambda environment.</param>
    /// <returns></returns>
    public void FunctionHandler(KafkaEvent evnt, ILambdaContext context)
    {

        foreach (var record in evnt.Records)
        {
            Console.WriteLine("Key:" + record.Key);
            foreach (var eventRecord in record.Value)
            {
                var valueBytes = eventRecord.Value.ToArray();
                var valueText = Encoding.UTF8.GetString(valueBytes);
```

```
                Console.WriteLine("Message:" + valueText);
            }
        }
    }


}
```

Go

Kit SDK pour Go V2

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement Amazon MSK avec Lambda en utilisant Go.

```
package main

import (
 "encoding/base64"
 "fmt"

 "github.com/aws/aws-lambda-go/events"
 "github.com/aws/aws-lambda-go/lambda"
)

func handler(event events.KafkaEvent) {
 for key, records := range event.Records {
  fmt.Println("Key:", key)

  for _, record := range records {
   fmt.Println("Record:", record)

   decodedValue, _ := base64.StdEncoding.DecodeString(record.Value)
   message := string(decodedValue)
```

```
   fmt.Println("Message:", message)
  }
 }
}

func main() {
 lambda.Start(handler)
}
```

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement Amazon MSK avec Lambda en utilisant Java.

```
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.KafkaEvent;
import com.amazonaws.services.lambda.runtime.events.KafkaEvent.KafkaEventRecord;

import java.util.Base64;
import java.util.Map;

public class Example implements RequestHandler<KafkaEvent, Void> {

    @Override
    public Void handleRequest(KafkaEvent event, Context context) {
        for (Map.Entry<String, java.util.List<KafkaEventRecord>> entry :
 event.getRecords().entrySet()) {
            String key = entry.getKey();
            System.out.println("Key: " + key);

            for (KafkaEventRecord record : entry.getValue()) {
                System.out.println("Record: " + record);
```

```
                byte[] value = Base64.getDecoder().decode(record.getValue());
                String message = new String(value);
                System.out.println("Message: " + message);
            }
        }

        return null;
    }
}
```

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement Amazon MSK avec Lambda à l'aide de JavaScript.

```
exports.handler = async (event) => {
    // Iterate through keys
    for (let key in event.records) {
      console.log('Key: ', key)
      // Iterate through records
      event.records[key].map((record) => {
        console.log('Record: ', record)
        // Decode base64
        const msg = Buffer.from(record.value, 'base64').toString()
        console.log('Message:', msg)
      })
    }
}
```

Consommation d'un événement Amazon MSK avec Lambda à l'aide de TypeScript.

```
import { MSKEvent, Context } from "aws-lambda";
```

```
import { Buffer } from "buffer";
import { Logger } from "@aws-lambda-powertools/logger";

const logger = new Logger({
  logLevel: "INFO",
  serviceName: "msk-handler-sample",
});

export const handler = async (
  event: MSKEvent,
  context: Context
): Promise<void> => {
  for (const [topic, topicRecords] of Object.entries(event.records)) {
    logger.info(`Processing key: ${topic}`);

    // Process each record in the partition
    for (const record of topicRecords) {
      try {
        // Decode the message value from base64
        const decodedMessage = Buffer.from(record.value, 'base64').toString();

        logger.info({
          message: decodedMessage
        });
      }
      catch (error) {
        logger.error('Error processing event', { error });
        throw error;
      }
    };
  }
}
```

PHP

Kit SDK pour PHP

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement Amazon MSK avec Lambda en utilisant PHP.

```
<?php
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0

// using bref/bref and bref/logger for simplicity

use Bref\Context\Context;
use Bref\Event\Kafka\KafkaEvent;
use Bref\Event\Handler as StdHandler;
use Bref\Logger\StderrLogger;

require __DIR__ . '/vendor/autoload.php';

class Handler implements StdHandler
{
    private StderrLogger $logger;
    public function __construct(StderrLogger $logger)
    {
        $this->logger = $logger;
    }

    /**
     * @throws JsonException
     * @throws \Bref\Event\InvalidLambdaEvent
     */
    public function handle(mixed $event, Context $context): void
    {
        $kafkaEvent = new KafkaEvent($event);
        $this->logger->info("Processing records");
        $records = $kafkaEvent->getRecords();
```

```
        foreach ($records as $record) {
            try {
                $key = $record->getKey();
                $this->logger->info("Key: $key");

                $values = $record->getValue();
                $this->logger->info(json_encode($values));

                foreach ($values as $value) {
                    $this->logger->info("Value: $value");
                }

            } catch (Exception $e) {
                $this->logger->error($e->getMessage());
            }
        }
        $totalRecords = count($records);
        $this->logger->info("Successfully processed $totalRecords records");
    }
}

$logger = new StderrLogger();
return new Handler($logger);
```

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement Amazon MSK avec Lambda en utilisant Python.

```
import base64

def lambda_handler(event, context):
    # Iterate through keys
```

```
    for key in event['records']:
        print('Key:', key)
        # Iterate through records
        for record in event['records'][key]:
            print('Record:', record)
            # Decode base64
            msg = base64.b64decode(record['value']).decode('utf-8')
            print('Message:', msg)
```

Ruby

Kit SDK pour Ruby

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement Amazon MSK avec Lambda en utilisant Ruby.

```
require 'base64'

def lambda_handler(event:, context:)
  # Iterate through keys
  event['records'].each do |key, records|
    puts "Key: #{key}"

    # Iterate through records
    records.each do |record|
      puts "Record: #{record}"

      # Decode base64
      msg = Base64.decode64(record['value'])
      puts "Message: #{msg}"
    end
  end
end
```

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement Amazon MSK avec Lambda en utilisant Rust.

```
use aws_lambda_events::event::kafka::KafkaEvent;
use lambda_runtime::{run, service_fn, tracing, Error, LambdaEvent};
use base64::prelude::*;
use serde_json::{Value};
use tracing::{info};

/// Pre-Requisites:
/// 1. Install Cargo Lambda - see https://www.cargo-lambda.info/guide/getting-
started.html
/// 2. Add packages tracing, tracing-subscriber, serde_json, base64
///
/// This is the main body for the function.
/// Write your code inside it.
/// There are some code example in the following URLs:
/// - https://github.com/awslabs/aws-lambda-rust-runtime/tree/main/examples
/// - https://github.com/aws-samples/serverless-rust-demo/

async fn function_handler(event: LambdaEvent<KafkaEvent>) -> Result<Value, Error>
 {

    let payload = event.payload.records;

    for (_name, records) in payload.iter() {

        for record in records {

         let record_text = record.value.as_ref().ok_or("Value is None")?;
         info!("Record: {}", &record_text);

         // perform Base64 decoding
         let record_bytes = BASE64_STANDARD.decode(record_text)?;
```

```
            let message = std::str::from_utf8(&record_bytes)?;

            info!("Message: {}", message);
          }

    }

    Ok(().into())
}

#[tokio::main]
async fn main() -> Result<(), Error> {

    // required to enable CloudWatch error logging by the runtime
    tracing::init_default_subscriber();
    info!("Setup CW subscriber!");

    run(service_fn(function_handler)).await
}
```

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Invoquer une fonction Lambda à partir d'un déclencheur Amazon S3

Les exemples de code suivants montrent comment implémenter une fonction Lambda qui reçoit un événement déclenché par le chargement d'un objet vers un compartiment S3. La fonction extrait le nom du compartiment S3 et la clé de l'objet à partir du paramètre d'événement et appelle l'API Amazon S3 pour récupérer et consigner le type de contenu de l'objet.

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Utilisation d'un événement S3 avec Lambda en utilisant .NET.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
using System.Threading.Tasks;
using Amazon.Lambda.Core;
using Amazon.S3;
using System;
using Amazon.Lambda.S3Events;
using System.Web;

// Assembly attribute to enable the Lambda function's JSON input to be converted
 into a .NET class.
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSeri

namespace S3Integration
{
    public class Function
    {
        private static AmazonS3Client _s3Client;
        public Function() : this(null)
        {
        }

        internal Function(AmazonS3Client s3Client)
        {
            _s3Client = s3Client ?? new AmazonS3Client();
        }

        public async Task<string> Handler(S3Event evt, ILambdaContext context)
        {
            try
            {
                if (evt.Records.Count <= 0)
                {
                    context.Logger.LogLine("Empty S3 Event received");
                    return string.Empty;
                }

                var bucket = evt.Records[0].S3.Bucket.Name;
                var key = HttpUtility.UrlDecode(evt.Records[0].S3.Object.Key);

                context.Logger.LogLine($"Request is for {bucket} and {key}");
```

```
                var objectResult = await _s3Client.GetObjectAsync(bucket, key);

                context.Logger.LogLine($"Returning {objectResult.Key}");

                return objectResult.Key;
            }
            catch (Exception e)
            {
                context.Logger.LogLine($"Error processing request -
 {e.Message}");

                return string.Empty;
            }
        }
    }
}
```

Go

Kit SDK pour Go V2

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Utilisation d'un événement S3 avec Lambda en utilisant Go.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package main

import (
 "context"
 "log"

 "github.com/aws/aws-lambda-go/events"
 "github.com/aws/aws-lambda-go/lambda"
 "github.com/aws/aws-sdk-go-v2/config"
 "github.com/aws/aws-sdk-go-v2/service/s3"
```

```
)

func handler(ctx context.Context, s3Event events.S3Event) error {
 sdkConfig, err := config.LoadDefaultConfig(ctx)
 if err != nil {
  log.Printf("failed to load default config: %s", err)
  return err
 }
 s3Client := s3.NewFromConfig(sdkConfig)

 for _, record := range s3Event.Records {
  bucket := record.S3.Bucket.Name
  key := record.S3.Object.URLDecodedKey
  headOutput, err := s3Client.HeadObject(ctx, &s3.HeadObjectInput{
   Bucket: &bucket,
   Key:    &key,
  })
  if err != nil {
   log.Printf("error getting head of object %s/%s: %s", bucket, key, err)
   return err
  }
  log.Printf("successfully retrieved %s/%s of type %s", bucket, key,
 *headOutput.ContentType)
 }

 return nil
}

func main() {
 lambda.Start(handler)
}
```

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Utilisation d'un événement S3 avec Lambda en utilisant Go.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package example;

import software.amazon.awssdk.services.s3.model.HeadObjectRequest;
import software.amazon.awssdk.services.s3.model.HeadObjectResponse;
import software.amazon.awssdk.services.s3.S3Client;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.S3Event;
import
 com.amazonaws.services.lambda.runtime.events.models.s3.S3EventNotification.S3EventNotifi

import org.slf4j.Logger;
import org.slf4j.LoggerFactory;

public class Handler implements RequestHandler<S3Event, String> {
    private static final Logger logger = LoggerFactory.getLogger(Handler.class);
    @Override
    public String handleRequest(S3Event s3event, Context context) {
        try {
          S3EventNotificationRecord record = s3event.getRecords().get(0);
          String srcBucket = record.getS3().getBucket().getName();
          String srcKey = record.getS3().getObject().getUrlDecodedKey();

          S3Client s3Client = S3Client.builder().build();
          HeadObjectResponse headObject = getHeadObject(s3Client, srcBucket,
 srcKey);

          logger.info("Successfully retrieved " + srcBucket + "/" + srcKey + " of
 type " + headObject.contentType());

          return "Ok";
        } catch (Exception e) {
          throw new RuntimeException(e);
        }
    }

    private HeadObjectResponse getHeadObject(S3Client s3Client, String bucket,
 String key) {
        HeadObjectRequest headObjectRequest = HeadObjectRequest.builder()
```

```
                .bucket(bucket)
                .key(key)
                .build();
        return s3Client.headObject(headObjectRequest);
    }
}
```

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement S3 avec Lambda en utilisant JavaScript.

```
import { S3Client, HeadObjectCommand } from "@aws-sdk/client-s3";

const client = new S3Client();

export const handler = async (event, context) => {

    // Get the object from the event and show its content type
    const bucket = event.Records[0].s3.bucket.name;
    const key = decodeURIComponent(event.Records[0].s3.object.key.replace(/\+/g,
 ' '));

    try {
        const { ContentType } = await client.send(new HeadObjectCommand({
            Bucket: bucket,
            Key: key,
        }));

        console.log('CONTENT TYPE:', ContentType);
        return ContentType;

    } catch (err) {
        console.log(err);
```

```
        const message = `Error getting object ${key} from bucket ${bucket}. Make
 sure they exist and your bucket is in the same region as this function.`;
        console.log(message);
        throw new Error(message);
    }
};
```

Consommation d'un événement S3 avec Lambda en utilisant TypeScript.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import { S3Event } from 'aws-lambda';
import { S3Client, HeadObjectCommand } from '@aws-sdk/client-s3';

const s3 = new S3Client({ region: process.env.AWS_REGION });

export const handler = async (event: S3Event): Promise<string | undefined> => {
  // Get the object from the event and show its content type
  const bucket = event.Records[0].s3.bucket.name;
  const key = decodeURIComponent(event.Records[0].s3.object.key.replace(/\+/g, '
 '));
  const params = {
    Bucket: bucket,
    Key: key,
  };
  try {
    const { ContentType } = await s3.send(new HeadObjectCommand(params));
    console.log('CONTENT TYPE:', ContentType);
    return ContentType;
  } catch (err) {
    console.log(err);
    const message = `Error getting object ${key} from bucket ${bucket}. Make sure
 they exist and your bucket is in the same region as this function.`;
    console.log(message);
    throw new Error(message);
  }
};
```

PHP

Kit SDK pour PHP

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement S3 avec Lambda à l'aide de PHP.

```
<?php

use Bref\Context\Context;
use Bref\Event\S3\S3Event;
use Bref\Event\S3\S3Handler;
use Bref\Logger\StderrLogger;

require __DIR__ . '/vendor/autoload.php';


class Handler extends S3Handler
{
    private StderrLogger $logger;
    public function __construct(StderrLogger $logger)
    {
        $this->logger = $logger;
    }

    public function handleS3(S3Event $event, Context $context) : void
    {
        $this->logger->info("Processing S3 records");

        // Get the object from the event and show its content type
        $records = $event->getRecords();

        foreach ($records as $record)
        {
            $bucket = $record->getBucket()->getName();
            $key = urldecode($record->getObject()->getKey());

            try {
```

```
                $fileSize = urldecode($record->getObject()->getSize());
                echo "File Size: " . $fileSize . "\n";
                // TODO: Implement your custom processing logic here
            } catch (Exception $e) {
                echo $e->getMessage() . "\n";
                echo 'Error getting object ' . $key . ' from bucket ' .
 $bucket . '. Make sure they exist and your bucket is in the same region as this
 function.' . "\n";
                throw $e;
            }
        }
    }
}

$logger = new StderrLogger();
return new Handler($logger);
```

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Utilisation d'un événement S3 avec Lambda en utilisant Python.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
import json
import urllib.parse
import boto3

print('Loading function')

s3 = boto3.client('s3')


def lambda_handler(event, context):
```

```
    #print("Received event: " + json.dumps(event, indent=2))

    # Get the object from the event and show its content type
    bucket = event['Records'][0]['s3']['bucket']['name']
    key = urllib.parse.unquote_plus(event['Records'][0]['s3']['object']['key'],
encoding='utf-8')
    try:
        response = s3.get_object(Bucket=bucket, Key=key)
        print("CONTENT TYPE: " + response['ContentType'])
        return response['ContentType']
    except Exception as e:
        print(e)
        print('Error getting object {} from bucket {}. Make sure they exist and
your bucket is in the same region as this function.'.format(key, bucket))
        raise e
```

Ruby

Kit SDK pour Ruby

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement S3 avec Lambda à l'aide de Ruby.

```
require 'json'
require 'uri'
require 'aws-sdk'

puts 'Loading function'

def lambda_handler(event:, context:)
  s3 = Aws::S3::Client.new(region: 'region') # Your AWS region
  # puts "Received event: #{JSON.dump(event)}"

  # Get the object from the event and show its content type
  bucket = event['Records'][0]['s3']['bucket']['name']
```

```
  key = URI.decode_www_form_component(event['Records'][0]['s3']['object']['key'],
 Encoding::UTF_8)
  begin
    response = s3.get_object(bucket: bucket, key: key)
    puts "CONTENT TYPE: #{response.content_type}"
    return response.content_type
  rescue StandardError => e
    puts e.message
    puts "Error getting object #{key} from bucket #{bucket}. Make sure they exist
 and your bucket is in the same region as this function."
    raise e
  end
end
```

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Utilisation d'un événement S3 avec Lambda en utilisant Rust.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
use aws_lambda_events::event::s3::S3Event;
use aws_sdk_s3::{Client};
use lambda_runtime::{run, service_fn, Error, LambdaEvent};


/// Main function
#[tokio::main]
async fn main() -> Result<(), Error> {
    tracing_subscriber::fmt()
        .with_max_level(tracing::Level::INFO)
        .with_target(false)
        .without_time()
        .init();
```

```
    // Initialize the AWS SDK for Rust
    let config = aws_config::load_from_env().await;
    let s3_client = Client::new(&config);

    let res = run(service_fn(|request: LambdaEvent<S3Event>| {
        function_handler(&s3_client, request)
    })).await;

    res
}

async fn function_handler(
    s3_client: &Client,
    evt: LambdaEvent<S3Event>
) -> Result<(), Error> {
    tracing::info!(records = ?evt.payload.records.len(), "Received request from
 SQS");

    if evt.payload.records.len() == 0 {
        tracing::info!("Empty S3 event received");
    }

    let bucket = evt.payload.records[0].s3.bucket.name.as_ref().expect("Bucket
 name to exist");
    let key = evt.payload.records[0].s3.object.key.as_ref().expect("Object key to
 exist");

    tracing::info!("Request is for {} and object {}", bucket, key);

    let s3_get_object_result = s3_client
        .get_object()
        .bucket(bucket)
        .key(key)
        .send()
        .await;

    match s3_get_object_result {
        Ok(_) => tracing::info!("S3 Get Object success, the s3GetObjectResult
 contains a 'body' property of type ByteStream"),
        Err(_) => tracing::info!("Failure with S3 Get Object request")
    }

    Ok(())
```

```
}
```

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Invocation d'une fonction lambda à partir d'un déclencheur Amazon SNS

Les exemples de code suivants montrent comment implémenter une fonction Lambda qui reçoit un événement déclenché par la réception de messages à partir d'une rubrique SNS. La fonction extrait les messages du paramètre d'événement et consigne le contenu de chaque message.

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement SNS avec Lambda à l'aide de .NET.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
using Amazon.Lambda.Core;
using Amazon.Lambda.SNSEvents;


// Assembly attribute to enable the Lambda function's JSON input to be converted
 into a .NET class.
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSeri

namespace SnsIntegration;

public class Function
{
    public async Task FunctionHandler(SNSEvent evnt, ILambdaContext context)
    {
```

```
        foreach (var record in evnt.Records)
        {
            await ProcessRecordAsync(record, context);
        }
        context.Logger.LogInformation("done");
    }

    private async Task ProcessRecordAsync(SNSEvent.SNSRecord record,
 ILambdaContext context)
    {
        try
        {
            context.Logger.LogInformation($"Processed record
 {record.Sns.Message}");

            // TODO: Do interesting work based on the new message
            await Task.CompletedTask;
        }
        catch (Exception e)
        {
            //You can use Dead Letter Queue to handle failures. By configuring a
 Lambda DLQ.
            context.Logger.LogError($"An error occurred");
            throw;
        }
    }
}
```

Go

Kit SDK pour Go V2

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement SNS avec Lambda à l'aide de Go.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
```

```
package main

import (
 "context"
 "fmt"

 "github.com/aws/aws-lambda-go/events"
 "github.com/aws/aws-lambda-go/lambda"
)

func handler(ctx context.Context, snsEvent events.SNSEvent) {
 for _, record := range snsEvent.Records {
  processMessage(record)
 }
 fmt.Println("done")
}

func processMessage(record events.SNSEventRecord) {
 message := record.SNS.Message
 fmt.Printf("Processed message: %s\n", message)
 // TODO: Process your record here
}

func main() {
 lambda.Start(handler)
}
```

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement SNS avec Lambda à l'aide de Java.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
```

```
package example;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.LambdaLogger;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.SNSEvent;
import com.amazonaws.services.lambda.runtime.events.SNSEvent.SNSRecord;


import java.util.Iterator;
import java.util.List;

public class SNSEventHandler implements RequestHandler<SNSEvent, Boolean> {
    LambdaLogger logger;

    @Override
    public Boolean handleRequest(SNSEvent event, Context context) {
        logger = context.getLogger();
        List<SNSRecord> records = event.getRecords();
        if (!records.isEmpty()) {
            Iterator<SNSRecord> recordsIter = records.iterator();
            while (recordsIter.hasNext()) {
                processRecord(recordsIter.next());
            }
        }
        return Boolean.TRUE;
    }

    public void processRecord(SNSRecord record) {
        try {
            String message = record.getSNS().getMessage();
            logger.log("message: " + message);
        } catch (Exception e) {
            throw new RuntimeException(e);
        }
    }

}
```

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement SNS avec Lambda à l'aide de JavaScript.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
exports.handler = async (event, context) => {
  for (const record of event.Records) {
    await processMessageAsync(record);
  }
  console.info("done");
};

async function processMessageAsync(record) {
  try {
    const message = JSON.stringify(record.Sns.Message);
    console.log(`Processed message ${message}`);
    await Promise.resolve(1); //Placeholder for actual async work
  } catch (err) {
    console.error("An error occurred");
    throw err;
  }
}
```

Consommation d'un événement SNS avec Lambda à l'aide de TypeScript.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import { SNSEvent, Context, SNSHandler, SNSEventRecord } from "aws-lambda";

export const functionHandler: SNSHandler = async (
  event: SNSEvent,
  context: Context
```

```
): Promise<void> => {
  for (const record of event.Records) {
    await processMessageAsync(record);
  }
  console.info("done");
};

async function processMessageAsync(record: SNSEventRecord): Promise<any> {
  try {
    const message: string = JSON.stringify(record.Sns.Message);
    console.log(`Processed message ${message}`);
    await Promise.resolve(1); //Placeholder for actual async work
  } catch (err) {
    console.error("An error occurred");
    throw err;
  }
}
```

PHP

Kit SDK pour PHP

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Utilisation d'un événement SNS avec Lambda à l'aide de PHP.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
<?php

/*
Since native PHP support for AWS Lambda is not available, we are utilizing Bref's
 PHP functions runtime for AWS Lambda.
For more information on Bref's PHP runtime for Lambda, refer to: https://bref.sh/
docs/runtimes/function

Another approach would be to create a custom runtime.
```

```
A practical example can be found here: https://aws.amazon.com/blogs/apn/aws-
lambda-custom-runtime-for-php-a-practical-example/
*/

// Additional composer packages may be required when using Bref or any other PHP
 functions runtime.
// require __DIR__ . '/vendor/autoload.php';

use Bref\Context\Context;
use Bref\Event\Sns\SnsEvent;
use Bref\Event\Sns\SnsHandler;

class Handler extends SnsHandler
{
    public function handleSns(SnsEvent $event, Context $context): void
    {
        foreach ($event->getRecords() as $record) {
            $message = $record->getMessage();

            // TODO: Implement your custom processing logic here
            // Any exception thrown will be logged and the invocation will be
 marked as failed

            echo "Processed Message: $message" . PHP_EOL;
        }
    }
}

return new Handler();
```

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Utilisation d'un événement SNS avec Lambda à l'aide de Python.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
def lambda_handler(event, context):
    for record in event['Records']:
        process_message(record)
    print("done")

def process_message(record):
    try:
        message = record['Sns']['Message']
        print(f"Processed message {message}")
        # TODO; Process your record here

    except Exception as e:
        print("An error occurred")
        raise e
```

Ruby

Kit SDK pour Ruby

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement SNS avec Lambda à l'aide de Ruby.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
def lambda_handler(event:, context:)
  event['Records'].map { |record| process_message(record) }
end

def process_message(record)
  message = record['Sns']['Message']
  puts("Processing message: #{message}")
rescue StandardError => e
  puts("Error processing message: #{e}")
```

```
  raise
end
```

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Utilisation d'un événement SNS avec Lambda à l'aide de Rust.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
use aws_lambda_events::event::sns::SnsEvent;
use aws_lambda_events::sns::SnsRecord;
use lambda_runtime::{run, service_fn, Error, LambdaEvent};
use tracing::info;

// Built with the following dependencies:
//  aws_lambda_events = { version = "0.10.0", default-features = false, features
 = ["sns"] }
//  lambda_runtime = "0.8.1"
//  tokio = { version = "1", features = ["macros"] }
//  tracing = { version = "0.1", features = ["log"] }
//  tracing-subscriber = { version = "0.3", default-features = false, features =
 ["fmt"] }

async fn function_handler(event: LambdaEvent<SnsEvent>) -> Result<(), Error> {
    for event in event.payload.records {
        process_record(&event)?;
    }

    Ok(())
}

fn process_record(record: &SnsRecord) -> Result<(), Error> {
    info!("Processing SNS Message: {}", record.sns.message);
```

```
    // Implement your record handling code here.

    Ok(())
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    tracing_subscriber::fmt()
        .with_max_level(tracing::Level::INFO)
        .with_target(false)
        .without_time()
        .init();

    run(service_fn(function_handler)).await
}
```

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Invoquer une fonction Lambda à partir d'un déclencheur Amazon SQS

Les exemples de code suivants montrent comment implémenter une fonction Lambda qui reçoit un événement déclenché par la réception de messages à partir d'une file d'attente SQS. La fonction extrait les messages du paramètre d'événement et consigne le contenu de chaque message.

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Utilisation d'un événement SQS avec Lambda en utilisant .NET.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
```

```
using Amazon.Lambda.Core;
using Amazon.Lambda.SQSEvents;


// Assembly attribute to enable the Lambda function's JSON input to be converted
 into a .NET class.
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSeri

namespace SqsIntegrationSampleCode
{
    public async Task FunctionHandler(SQSEvent evnt, ILambdaContext context)
    {
        foreach (var message in evnt.Records)
        {
            await ProcessMessageAsync(message, context);
        }

        context.Logger.LogInformation("done");
    }

    private async Task ProcessMessageAsync(SQSEvent.SQSMessage message,
 ILambdaContext context)
    {
        try
        {
            context.Logger.LogInformation($"Processed message {message.Body}");

            // TODO: Do interesting work based on the new message
            await Task.CompletedTask;
        }
        catch (Exception e)
        {
            //You can use Dead Letter Queue to handle failures. By configuring a
 Lambda DLQ.
            context.Logger.LogError($"An error occurred");
            throw;
        }

    }
}
```

Go

Kit SDK pour Go V2

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement SQS avec Lambda à l'aide de Go.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package integration_sqs_to_lambda

import (
 "fmt"
 "github.com/aws/aws-lambda-go/events"
 "github.com/aws/aws-lambda-go/lambda"
)

func handler(event events.SQSEvent) error {
 for _, record := range event.Records {
  err := processMessage(record)
  if err != nil {
   return err
  }
 }
 fmt.Println("done")
 return nil
}

func processMessage(record events.SQSMessage) error {
 fmt.Printf("Processed message %s\n", record.Body)
 // TODO: Do interesting work based on the new message
 return nil
}

func main() {
 lambda.Start(handler)
}
```

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Utilisation d'un événement SQS avec Lambda à l'aide de Java.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.SQSEvent;
import com.amazonaws.services.lambda.runtime.events.SQSEvent.SQSMessage;

public class Function implements RequestHandler<SQSEvent, Void> {
    @Override
    public Void handleRequest(SQSEvent sqsEvent, Context context) {
        for (SQSMessage msg : sqsEvent.getRecords()) {
            processMessage(msg, context);
        }
        context.getLogger().log("done");
        return null;
    }

    private void processMessage(SQSMessage msg, Context context) {
        try {
            context.getLogger().log("Processed message " + msg.getBody());

            // TODO: Do interesting work based on the new message

        } catch (Exception e) {
            context.getLogger().log("An error occurred");
            throw e;
        }
```

```
    }
}
```

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement SQS avec Lambda à l'aide de JavaScript.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
exports.handler = async (event, context) => {
  for (const message of event.Records) {
    await processMessageAsync(message);
  }
  console.info("done");
};

async function processMessageAsync(message) {
  try {
    console.log(`Processed message ${message.body}`);
    // TODO: Do interesting work based on the new message
    await Promise.resolve(1); //Placeholder for actual async work
  } catch (err) {
    console.error("An error occurred");
    throw err;
  }
}
```

Consommation d'un événement SQS avec Lambda à l'aide de TypeScript.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import { SQSEvent, Context, SQSHandler, SQSRecord } from "aws-lambda";
```

```
export const functionHandler: SQSHandler = async (
  event: SQSEvent,
  context: Context
): Promise<void> => {
  for (const message of event.Records) {
    await processMessageAsync(message);
  }
  console.info("done");
};

async function processMessageAsync(message: SQSRecord): Promise<any> {
  try {
    console.log(`Processed message ${message.body}`);
    // TODO: Do interesting work based on the new message
    await Promise.resolve(1); //Placeholder for actual async work
  } catch (err) {
    console.error("An error occurred");
    throw err;
  }
}
```

PHP

Kit SDK pour PHP

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement SQS avec Lambda à l'aide de PHP.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
<?php

# using bref/bref and bref/logger for simplicity

use Bref\Context\Context;
```

```
use Bref\Event\InvalidLambdaEvent;
use Bref\Event\Sqs\SqsEvent;
use Bref\Event\Sqs\SqsHandler;
use Bref\Logger\StderrLogger;

require __DIR__ . '/vendor/autoload.php';

class Handler extends SqsHandler
{
    private StderrLogger $logger;
    public function __construct(StderrLogger $logger)
    {
        $this->logger = $logger;
    }

    /**
     * @throws InvalidLambdaEvent
     */
    public function handleSqs(SqsEvent $event, Context $context): void
    {
        foreach ($event->getRecords() as $record) {
            $body = $record->getBody();
            // TODO: Do interesting work based on the new message
        }
    }
}

$logger = new StderrLogger();
return new Handler($logger);
```

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Utilisation d'un événement SQS avec Lambda à l'aide de Python.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
def lambda_handler(event, context):
    for message in event['Records']:
        process_message(message)
    print("done")

def process_message(message):
    try:
        print(f"Processed message {message['body']}")
        # TODO: Do interesting work based on the new message
    except Exception as err:
        print("An error occurred")
        raise err
```

Ruby

Kit SDK pour Ruby

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Utilisation d'un événement SQS avec Lambda à l'aide de Ruby.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
def lambda_handler(event:, context:)
  event['Records'].each do |message|
    process_message(message)
  end
  puts "done"
end

def process_message(message)
  begin
    puts "Processed message #{message['body']}"
    # TODO: Do interesting work based on the new message
```

```
  rescue StandardError => err
    puts "An error occurred"
    raise err
  end
end
```

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Consommation d'un événement SQS avec Lambda à l'aide de Rust.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
use aws_lambda_events::event::sqs::SqsEvent;
use lambda_runtime::{run, service_fn, Error, LambdaEvent};

async fn function_handler(event: LambdaEvent<SqsEvent>) -> Result<(), Error> {
    event.payload.records.iter().for_each(|record| {
        // process the record
        tracing::info!("Message body: {}",
 record.body.as_deref().unwrap_or_default())
    });

    Ok(())
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    tracing_subscriber::fmt()
        .with_max_level(tracing::Level::INFO)
        // disable printing the name of the module in every log line.
        .with_target(false)
        // disabling time is handy because CloudWatch will add the ingestion
 time.
        .without_time()
```

```
        .init();

    run(service_fn(function_handler)).await
}
```

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Signalement des échecs d'articles par lots pour les fonctions Lambda à l'aide d'un déclencheur Kinesis

Les exemples de code suivants montrent comment implémenter une réponse par lots partielle pour les fonctions Lambda qui reçoivent des événements d'un flux Kinesis. La fonction signale les défaillances échecs d'articles par lots dans la réponse, en indiquant à Lambda de réessayer ces messages ultérieurement.

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signalement des échecs d'articles par lots Kinesis avec Lambda à l'aide de .NET.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
using System.Text;
using System.Text.Json.Serialization;
using Amazon.Lambda.Core;
using Amazon.Lambda.KinesisEvents;
using AWS.Lambda.Powertools.Logging;

// Assembly attribute to enable the Lambda function's JSON input to be converted
 into a .NET class.
```

```
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSeri

namespace KinesisIntegration;

public class Function
{
    // Powertools Logger requires an environment variables against your function
    // POWERTOOLS_SERVICE_NAME
    [Logging(LogEvent = true)]
    public async Task<StreamsEventResponse> FunctionHandler(KinesisEvent evnt,
 ILambdaContext context)
    {
        if (evnt.Records.Count == 0)
        {
            Logger.LogInformation("Empty Kinesis Event received");
            return new StreamsEventResponse();
        }

        foreach (var record in evnt.Records)
        {
            try
            {
                Logger.LogInformation($"Processed Event with EventId:
 {record.EventId}");
                string data = await GetRecordDataAsync(record.Kinesis, context);
                Logger.LogInformation($"Data: {data}");
                // TODO: Do interesting work based on the new data
            }
            catch (Exception ex)
            {
                Logger.LogError($"An error occurred {ex.Message}");
                /* Since we are working with streams, we can return the failed
 item immediately.
                   Lambda will immediately begin to retry processing from this
 failed item onwards. */
                return new StreamsEventResponse
                {
                    BatchItemFailures = new
 List<StreamsEventResponse.BatchItemFailure>
                    {
                        new StreamsEventResponse.BatchItemFailure
 { ItemIdentifier = record.Kinesis.SequenceNumber }
                    }
```

```
                };
            }
        }
        Logger.LogInformation($"Successfully processed {evnt.Records.Count}
 records.");
        return new StreamsEventResponse();
    }

    private async Task<string> GetRecordDataAsync(KinesisEvent.Record record,
 ILambdaContext context)
    {
        byte[] bytes = record.Data.ToArray();
        string data = Encoding.UTF8.GetString(bytes);
        await Task.CompletedTask; //Placeholder for actual async work
        return data;
    }
}

public class StreamsEventResponse
{
    [JsonPropertyName("batchItemFailures")]
    public IList<BatchItemFailure> BatchItemFailures { get; set; }
    public class BatchItemFailure
    {
        [JsonPropertyName("itemIdentifier")]
        public string ItemIdentifier { get; set; }
    }
}
```

Go

Kit SDK pour Go V2

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signalement des échecs d'articles par lots Kinesis avec Lambda à l'aide de Go.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
```

```
// SPDX-License-Identifier: Apache-2.0
package main

import (
 "context"
 "fmt"
 "github.com/aws/aws-lambda-go/events"
 "github.com/aws/aws-lambda-go/lambda"
)

func handler(ctx context.Context, kinesisEvent events.KinesisEvent)
 (map[string]interface{}, error) {
 batchItemFailures := []map[string]interface{}{}

 for _, record := range kinesisEvent.Records {
  curRecordSequenceNumber := ""

  // Process your record
  if /* Your record processing condition here */ {
   curRecordSequenceNumber = record.Kinesis.SequenceNumber
  }

  // Add a condition to check if the record processing failed
  if curRecordSequenceNumber != "" {
   batchItemFailures = append(batchItemFailures, map[string]interface{}
{"itemIdentifier": curRecordSequenceNumber})
  }
 }

 kinesisBatchResponse := map[string]interface{}{
  "batchItemFailures": batchItemFailures,
 }
 return kinesisBatchResponse, nil
}

func main() {
 lambda.Start(handler)
}
```

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signalement des échecs d'articles par lots Kinesis avec Lambda à l'aide de Java.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.KinesisEvent;
import com.amazonaws.services.lambda.runtime.events.StreamsEventResponse;

import java.io.Serializable;
import java.util.ArrayList;
import java.util.List;

public class ProcessKinesisRecords implements RequestHandler<KinesisEvent,
 StreamsEventResponse> {

    @Override
    public StreamsEventResponse handleRequest(KinesisEvent input, Context
 context) {

        List<StreamsEventResponse.BatchItemFailure> batchItemFailures = new
 ArrayList<>();
        String curRecordSequenceNumber = "";

        for (KinesisEvent.KinesisEventRecord kinesisEventRecord :
 input.getRecords()) {
            try {
                //Process your record
                KinesisEvent.Record kinesisRecord =
 kinesisEventRecord.getKinesis();
                curRecordSequenceNumber = kinesisRecord.getSequenceNumber();

            } catch (Exception e) {
```

```
                /* Since we are working with streams, we can return the failed
 item immediately.
                   Lambda will immediately begin to retry processing from this
 failed item onwards. */
                batchItemFailures.add(new
 StreamsEventResponse.BatchItemFailure(curRecordSequenceNumber));
                return new StreamsEventResponse(batchItemFailures);
            }
        }

       return new StreamsEventResponse(batchItemFailures);
    }
}
```

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signalement des échecs d'articles par lots Kinesis avec Lambda à l'aide de JavaScript.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
exports.handler = async (event, context) => {
  for (const record of event.Records) {
    try {
      console.log(`Processed Kinesis Event - EventID: ${record.eventID}`);
      const recordData = await getRecordDataAsync(record.kinesis);
      console.log(`Record Data: ${recordData}`);
      // TODO: Do interesting work based on the new data
    } catch (err) {
      console.error(`An error occurred ${err}`);
      /* Since we are working with streams, we can return the failed item
 immediately.
           Lambda will immediately begin to retry processing from this failed
 item onwards. */
```

```
      return {
        batchItemFailures: [{ itemIdentifier: record.kinesis.sequenceNumber }],
      };
    }
  }
  console.log(`Successfully processed ${event.Records.length} records.`);
  return { batchItemFailures: [] };
};

async function getRecordDataAsync(payload) {
  var data = Buffer.from(payload.data, "base64").toString("utf-8");
  await Promise.resolve(1); //Placeholder for actual async work
  return data;
}
```

Signaler les défaillances d'un lot Kinesis avec Lambda à l'aide de TypeScript.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import {
  KinesisStreamEvent,
  Context,
  KinesisStreamHandler,
  KinesisStreamRecordPayload,
  KinesisStreamBatchResponse,
} from "aws-lambda";
import { Buffer } from "buffer";
import { Logger } from "@aws-lambda-powertools/logger";

const logger = new Logger({
  logLevel: "INFO",
  serviceName: "kinesis-stream-handler-sample",
});

export const functionHandler: KinesisStreamHandler = async (
  event: KinesisStreamEvent,
  context: Context
): Promise<KinesisStreamBatchResponse> => {
  for (const record of event.Records) {
    try {
      logger.info(`Processed Kinesis Event - EventID: ${record.eventID}`);
      const recordData = await getRecordDataAsync(record.kinesis);
```

```
      logger.info(`Record Data: ${recordData}`);
      // TODO: Do interesting work based on the new data
    } catch (err) {
      logger.error(`An error occurred ${err}`);
      /* Since we are working with streams, we can return the failed item
 immediately.
           Lambda will immediately begin to retry processing from this failed
 item onwards. */
      return {
        batchItemFailures: [{ itemIdentifier: record.kinesis.sequenceNumber }],
      };
    }
  }
  logger.info(`Successfully processed ${event.Records.length} records.`);
  return { batchItemFailures: [] };
};

async function getRecordDataAsync(
  payload: KinesisStreamRecordPayload
): Promise<string> {
  var data = Buffer.from(payload.data, "base64").toString("utf-8");
  await Promise.resolve(1); //Placeholder for actual async work
  return data;
}
```

PHP

Kit SDK pour PHP

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signalement des échecs d'articles par lots Kinesis avec Lambda à l'aide de PHP.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
<?php
```

```
# using bref/bref and bref/logger for simplicity

use Bref\Context\Context;
use Bref\Event\Kinesis\KinesisEvent;
use Bref\Event\Handler as StdHandler;
use Bref\Logger\StderrLogger;

require __DIR__ . '/vendor/autoload.php';

class Handler implements StdHandler
{
    private StderrLogger $logger;
    public function __construct(StderrLogger $logger)
    {
        $this->logger = $logger;
    }

    /**
     * @throws JsonException
     * @throws \Bref\Event\InvalidLambdaEvent
     */
    public function handle(mixed $event, Context $context): array
    {
        $kinesisEvent = new KinesisEvent($event);
        $this->logger->info("Processing records");
        $records = $kinesisEvent->getRecords();

        $failedRecords = [];
        foreach ($records as $record) {
            try {
                $data = $record->getData();
                $this->logger->info(json_encode($data));
                // TODO: Do interesting work based on the new data
            } catch (Exception $e) {
                $this->logger->error($e->getMessage());
                // failed processing the record
                $failedRecords[] = $record->getSequenceNumber();
            }
        }
        $totalRecords = count($records);
        $this->logger->info("Successfully processed $totalRecords records");

        // change format for the response
        $failures = array_map(
```

```
            fn(string $sequenceNumber) => ['itemIdentifier' => $sequenceNumber],
            $failedRecords
        );

        return [
            'batchItemFailures' => $failures
        ];
    }
}

$logger = new StderrLogger();
return new Handler($logger);
```

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signalement des échecs d'articles par lots Kinesis avec Lambda à l'aide de Python.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
def handler(event, context):
    records = event.get("Records")
    curRecordSequenceNumber = ""

    for record in records:
        try:
            # Process your record
            curRecordSequenceNumber = record["kinesis"]["sequenceNumber"]
        except Exception as e:
            # Return failed record's sequence number
            return {"batchItemFailures":[{"itemIdentifier":
 curRecordSequenceNumber}]}

    return {"batchItemFailures":[]}
```

Ruby

Kit SDK pour Ruby

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signalement des échecs d'articles par lots Kinesis avec Lambda à l'aide de Ruby.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
require 'aws-sdk'

def lambda_handler(event:, context:)
  batch_item_failures = []

  event['Records'].each do |record|
    begin
      puts "Processed Kinesis Event - EventID: #{record['eventID']}"
      record_data = get_record_data_async(record['kinesis'])
      puts "Record Data: #{record_data}"
      # TODO: Do interesting work based on the new data
    rescue StandardError => err
      puts "An error occurred #{err}"
      # Since we are working with streams, we can return the failed item
 immediately.
      # Lambda will immediately begin to retry processing from this failed item
 onwards.
      return { batchItemFailures: [{ itemIdentifier: record['kinesis']
['sequenceNumber'] }] }
    end
  end

  puts "Successfully processed #{event['Records'].length} records."
  { batchItemFailures: batch_item_failures }
end
```

```
def get_record_data_async(payload)
  data = Base64.decode64(payload['data']).force_encoding('utf-8')
  # Placeholder for actual async work
  sleep(1)
  data
end
```

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signalement des échecs d'articles par lots Kinesis avec Lambda à l'aide de Rust.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
use aws_lambda_events::{
    event::kinesis::KinesisEvent,
    kinesis::KinesisEventRecord,
    streams::{KinesisBatchItemFailure, KinesisEventResponse},
};
use lambda_runtime::{run, service_fn, Error, LambdaEvent};

async fn function_handler(event: LambdaEvent<KinesisEvent>) ->
 Result<KinesisEventResponse, Error> {
    let mut response = KinesisEventResponse {
        batch_item_failures: vec![],
    };

    if event.payload.records.is_empty() {
        tracing::info!("No records found. Exiting.");
        return Ok(response);
    }

    for record in &event.payload.records {
        tracing::info!(
            "EventId: {}",
```

```
            record.event_id.as_deref().unwrap_or_default()
        );

        let record_processing_result = process_record(record);

        if record_processing_result.is_err() {
            response.batch_item_failures.push(KinesisBatchItemFailure {
                item_identifier: record.kinesis.sequence_number.clone(),
            });
            /* Since we are working with streams, we can return the failed item
 immediately.
            Lambda will immediately begin to retry processing from this failed
 item onwards. */
            return Ok(response);
        }
    }

    tracing::info!(
        "Successfully processed {} records",
        event.payload.records.len()
    );

    Ok(response)
}

fn process_record(record: &KinesisEventRecord) -> Result<(), Error> {
    let record_data = std::str::from_utf8(record.kinesis.data.as_slice());

    if let Some(err) = record_data.err() {
        tracing::error!("Error: {}", err);
        return Err(Error::from(err));
    }

    let record_data = record_data.unwrap_or_default();

    // do something interesting with the data
    tracing::info!("Data: {}", record_data);

    Ok(())
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    tracing_subscriber::fmt()
```

```
        .with_max_level(tracing::Level::INFO)
        // disable printing the name of the module in every log line.
        .with_target(false)
        // disabling time is handy because CloudWatch will add the ingestion
 time.
        .without_time()
        .init();

    run(service_fn(function_handler)).await
}
```

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Signalement des échecs d'articles par lots pour les fonctions Lambda à l'aide d'un déclencheur DynamoDB

Les exemples de code suivants illustrent comment implémenter une réponse partielle par lots pour les fonctions Lambda qui reçoivent des événements à partir d'un flux DynamoDB. La fonction signale les défaillances échecs d'articles par lots dans la réponse, en indiquant à Lambda de réessayer ces messages ultérieurement.

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signalement des échecs d'articles par lots DynamoDB avec Lambda à l'aide de .NET.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
using System.Text.Json;
using System.Text;
using Amazon.Lambda.Core;
```

```
using Amazon.Lambda.DynamoDBEvents;

// Assembly attribute to enable the Lambda function's JSON input to be converted
 into a .NET class.
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSeri

namespace AWSLambda_DDB;

public class Function
{
    public StreamsEventResponse FunctionHandler(DynamoDBEvent dynamoEvent,
 ILambdaContext context)

    {
        context.Logger.LogInformation($"Beginning to process
 {dynamoEvent.Records.Count} records...");
        List<StreamsEventResponse.BatchItemFailure> batchItemFailures = new
 List<StreamsEventResponse.BatchItemFailure>();
        StreamsEventResponse streamsEventResponse = new StreamsEventResponse();

        foreach (var record in dynamoEvent.Records)
        {
            try
            {
                var sequenceNumber = record.Dynamodb.SequenceNumber;
                context.Logger.LogInformation(sequenceNumber);
            }
            catch (Exception ex)
            {
                context.Logger.LogError(ex.Message);
                batchItemFailures.Add(new StreamsEventResponse.BatchItemFailure()
 { ItemIdentifier = record.Dynamodb.SequenceNumber });
            }
        }

        if (batchItemFailures.Count > 0)
        {
            streamsEventResponse.BatchItemFailures = batchItemFailures;
        }

        context.Logger.LogInformation("Stream processing complete.");
        return streamsEventResponse;
    }
```

```
}
```

Go

Kit SDK pour Go V2

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signalement des échecs d'articles par lots DynamoDB avec Lambda à l'aide de Go.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package main

import (
 "context"
 "github.com/aws/aws-lambda-go/events"
 "github.com/aws/aws-lambda-go/lambda"
)

type BatchItemFailure struct {
 ItemIdentifier string `json:"ItemIdentifier"`
}

type BatchResult struct {
 BatchItemFailures []BatchItemFailure `json:"BatchItemFailures"`
}

func HandleRequest(ctx context.Context, event events.DynamoDBEvent)
 (*BatchResult, error) {
 var batchItemFailures []BatchItemFailure
 curRecordSequenceNumber := ""

 for _, record := range event.Records {
  // Process your record
  curRecordSequenceNumber = record.Change.SequenceNumber
 }
```

```
 if curRecordSequenceNumber != "" {
  batchItemFailures = append(batchItemFailures, BatchItemFailure{ItemIdentifier:
 curRecordSequenceNumber})
 }

 batchResult := BatchResult{
  BatchItemFailures: batchItemFailures,
 }

 return &batchResult, nil
}

func main() {
 lambda.Start(HandleRequest)
}
```

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signalement des échecs d'articles par lots DynamoDB avec Lambda à l'aide de Java.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.DynamodbEvent;
import com.amazonaws.services.lambda.runtime.events.StreamsEventResponse;
import com.amazonaws.services.lambda.runtime.events.models.dynamodb.StreamRecord;

import java.util.ArrayList;
import java.util.List;

public class ProcessDynamodbRecords implements RequestHandler<DynamodbEvent,
 StreamsEventResponse> {
```

```
    @Override
    public StreamsEventResponse handleRequest(DynamodbEvent input, Context
 context) {

        List<StreamsEventResponse.BatchItemFailure> batchItemFailures = new
 ArrayList<>();
        String curRecordSequenceNumber = "";

        for (DynamodbEvent.DynamodbStreamRecord dynamodbStreamRecord :
 input.getRecords()) {
          try {
                //Process your record
                StreamRecord dynamodbRecord = dynamodbStreamRecord.getDynamodb();
                curRecordSequenceNumber = dynamodbRecord.getSequenceNumber();

            } catch (Exception e) {
                /* Since we are working with streams, we can return the failed
 item immediately.
                   Lambda will immediately begin to retry processing from this
 failed item onwards. */
                batchItemFailures.add(new
 StreamsEventResponse.BatchItemFailure(curRecordSequenceNumber));
                return new StreamsEventResponse(batchItemFailures);
            }
        }

       return new StreamsEventResponse();
    }
}
```

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signaler les défaillances d'éléments de lot DynamoDB avec Lambda à l'aide de JavaScript.

```
export const handler = async (event) => {
  const records = event.Records;
  let curRecordSequenceNumber = "";

  for (const record of records) {
    try {
      // Process your record
      curRecordSequenceNumber = record.dynamodb.SequenceNumber;
    } catch (e) {
      // Return failed record's sequence number
      return { batchItemFailures: [{ itemIdentifier:
 curRecordSequenceNumber }] };
    }
  }

  return { batchItemFailures: [] };
};
```

Signaler les défaillances d'éléments de lot DynamoDB avec Lambda à l'aide de TypeScript.

```
import {
  DynamoDBBatchResponse,
  DynamoDBBatchItemFailure,
  DynamoDBStreamEvent,
} from "aws-lambda";

export const handler = async (
  event: DynamoDBStreamEvent
): Promise<DynamoDBBatchResponse> => {
  const batchItemFailures: DynamoDBBatchItemFailure[] = [];
  let curRecordSequenceNumber;

  for (const record of event.Records) {
    curRecordSequenceNumber = record.dynamodb?.SequenceNumber;

    if (curRecordSequenceNumber) {
      batchItemFailures.push({
        itemIdentifier: curRecordSequenceNumber,
      });
    }
```

```
  }

  return { batchItemFailures: batchItemFailures };
};
```

PHP

Kit SDK pour PHP

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signalement des échecs d'articles par lots DynamoDB avec Lambda à l'aide de PHP.

```
<?php

# using bref/bref and bref/logger for simplicity

use Bref\Context\Context;
use Bref\Event\DynamoDb\DynamoDbEvent;
use Bref\Event\Handler as StdHandler;
use Bref\Logger\StderrLogger;

require __DIR__ . '/vendor/autoload.php';

class Handler implements StdHandler
{
    private StderrLogger $logger;
    public function __construct(StderrLogger $logger)
    {
        $this->logger = $logger;
    }

    /**
     * @throws JsonException
     * @throws \Bref\Event\InvalidLambdaEvent
     */
    public function handle(mixed $event, Context $context): array
```

```
    {
        $dynamoDbEvent = new DynamoDbEvent($event);
        $this->logger->info("Processing records");

        $records = $dynamoDbEvent->getRecords();
        $failedRecords = [];
        foreach ($records as $record) {
            try {
                $data = $record->getData();
                $this->logger->info(json_encode($data));
                // TODO: Do interesting work based on the new data
            } catch (Exception $e) {
                $this->logger->error($e->getMessage());
                // failed processing the record
                $failedRecords[] = $record->getSequenceNumber();
            }
        }
        $totalRecords = count($records);
        $this->logger->info("Successfully processed $totalRecords records");

        // change format for the response
        $failures = array_map(
            fn(string $sequenceNumber) => ['itemIdentifier' => $sequenceNumber],
            $failedRecords
        );

        return [
            'batchItemFailures' => $failures
        ];
    }
}

$logger = new StderrLogger();
return new Handler($logger);
```

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signalement des échecs d'articles par lots DynamoDB avec Lambda à l'aide de Python.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
def handler(event, context):
    records = event.get("Records")
    curRecordSequenceNumber = ""

    for record in records:
        try:
            # Process your record
            curRecordSequenceNumber = record["dynamodb"]["SequenceNumber"]
        except Exception as e:
            # Return failed record's sequence number
            return {"batchItemFailures":[{"itemIdentifier":
 curRecordSequenceNumber}]}

    return {"batchItemFailures":[]}
```

Ruby

Kit SDK pour Ruby

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signalement des échecs d'articles par lots DynamoDB avec Lambda à l'aide de Ruby.

```
def lambda_handler(event:, context:)
    records = event["Records"]
    cur_record_sequence_number = ""

    records.each do |record|
      begin
        # Process your record
        cur_record_sequence_number = record["dynamodb"]["SequenceNumber"]
      rescue StandardError => e
        # Return failed record's sequence number
        return {"batchItemFailures" => [{"itemIdentifier" =>
 cur_record_sequence_number}]}
      end
    end

    {"batchItemFailures" => []}
  end
```

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signalement des échecs d'articles par lots DynamoDB avec Lambda à l'aide de Rust.

```
use aws_lambda_events::{
    event::dynamodb::{Event, EventRecord, StreamRecord},
    streams::{DynamoDbBatchItemFailure, DynamoDbEventResponse},
};
use lambda_runtime::{run, service_fn, Error, LambdaEvent};

/// Process the stream record
fn process_record(record: &EventRecord) -> Result<(), Error> {
    let stream_record: &StreamRecord = &record.change;
```

```
    // process your stream record here...
    tracing::info!("Data: {:?}", stream_record);

    Ok(())
}

/// Main Lambda handler here...
async fn function_handler(event: LambdaEvent<Event>) ->
 Result<DynamoDbEventResponse, Error> {
    let mut response = DynamoDbEventResponse {
        batch_item_failures: vec![],
    };

    let records = &event.payload.records;

    if records.is_empty() {
        tracing::info!("No records found. Exiting.");
        return Ok(response);
    }

    for record in records {
        tracing::info!("EventId: {}", record.event_id);

        // Couldn't find a sequence number
        if record.change.sequence_number.is_none() {
            response.batch_item_failures.push(DynamoDbBatchItemFailure {
                item_identifier: Some("".to_string()),
            });
            return Ok(response);
        }

        // Process your record here...
        if process_record(record).is_err() {
            response.batch_item_failures.push(DynamoDbBatchItemFailure {
                item_identifier: record.change.sequence_number.clone(),
            });
            /* Since we are working with streams, we can return the failed item
 immediately.
            Lambda will immediately begin to retry processing from this failed
 item onwards. */
            return Ok(response);
        }
    }
```

```
    tracing::info!("Successfully processed {} record(s)", records.len());

    Ok(response)
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    tracing_subscriber::fmt()
        .with_max_level(tracing::Level::INFO)
        // disable printing the name of the module in every log line.
        .with_target(false)
        // disabling time is handy because CloudWatch will add the ingestion
 time.
        .without_time()
        .init();

    run(service_fn(function_handler)).await
}
```

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Signalement des échecs d'articles par lots pour les fonctions Lambda à l'aide d'un déclencheur Amazon SQS

Les exemples de code suivants montrent comment implémenter une réponse par lots partielle pour les fonctions Lambda qui reçoivent des événements d'une file d'attente SQS. La fonction signale les défaillances échecs d'articles par lots dans la réponse, en indiquant à Lambda de réessayer ces messages ultérieurement.

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signalement des échecs d'articles par lots SQS avec Lambda à l'aide de .NET.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
using Amazon.Lambda.Core;
using Amazon.Lambda.SQSEvents;

// Assembly attribute to enable the Lambda function's JSON input to be converted
 into a .NET class.
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSeri
namespace sqsSample;

public class Function
{
    public async Task<SQSBatchResponse> FunctionHandler(SQSEvent evnt,
 ILambdaContext context)
    {
        List<SQSBatchResponse.BatchItemFailure> batchItemFailures = new
 List<SQSBatchResponse.BatchItemFailure>();
        foreach(var message in evnt.Records)
        {
            try
            {
                //process your message
                await ProcessMessageAsync(message, context);
            }
            catch (System.Exception)
            {
                //Add failed message identifier to the batchItemFailures list
                batchItemFailures.Add(new
 SQSBatchResponse.BatchItemFailure{ItemIdentifier=message.MessageId});
            }
```

```
        }
        return new SQSBatchResponse(batchItemFailures);
    }

    private async Task ProcessMessageAsync(SQSEvent.SQSMessage message,
 ILambdaContext context)
    {
        if (String.IsNullOrEmpty(message.Body))
        {
            throw new Exception("No Body in SQS Message.");
        }
        context.Logger.LogInformation($"Processed message {message.Body}");
        // TODO: Do interesting work based on the new message
        await Task.CompletedTask;
    }
}
```

Go

Kit SDK pour Go V2

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signalement des échecs d'articles par lots SQS avec Lambda à l'aide de Go.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package main

import (
 "context"
 "fmt"
 "github.com/aws/aws-lambda-go/events"
 "github.com/aws/aws-lambda-go/lambda"
)

func handler(ctx context.Context, sqsEvent events.SQSEvent)
 (map[string]interface{}, error) {
```

```
 batchItemFailures := []map[string]interface{}{}

 for _, message := range sqsEvent.Records {
  if len(message.Body) > 0 {
   // Your message processing condition here
   fmt.Printf("Successfully processed message: %s\n", message.Body)
  } else {
   // Message processing failed
   fmt.Printf("Failed to process message %s\n", message.MessageId)
   batchItemFailures = append(batchItemFailures, map[string]interface{}
{"itemIdentifier": message.MessageId})
  }
 }

 sqsBatchResponse := map[string]interface{}{
  "batchItemFailures": batchItemFailures,
 }
 return sqsBatchResponse, nil
}

func main() {
 lambda.Start(handler)
}
```

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signalement des échecs d'articles par lots SQS avec Lambda à l'aide de Java.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.SQSEvent;
```

```
import com.amazonaws.services.lambda.runtime.events.SQSBatchResponse;

import java.util.ArrayList;
import java.util.List;

public class ProcessSQSMessageBatch implements RequestHandler<SQSEvent,
 SQSBatchResponse> {
    @Override
    public SQSBatchResponse handleRequest(SQSEvent sqsEvent, Context context) {
         List<SQSBatchResponse.BatchItemFailure> batchItemFailures = new
 ArrayList<SQSBatchResponse.BatchItemFailure>();

         for (SQSEvent.SQSMessage message : sqsEvent.getRecords()) {
             try {
                 //process your message
             } catch (Exception e) {
                 //Add failed message identifier to the batchItemFailures list
                 batchItemFailures.add(new
 SQSBatchResponse.BatchItemFailure(message.getMessageId()));
             }
         }
         return new SQSBatchResponse(batchItemFailures);
     }
}
```

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signaler les défaillances d'articles par lots SQS avec Lambda à l'aide de JavaScript.

```
// Node.js 20.x Lambda runtime, AWS SDK for Javascript V3
export const handler = async (event, context) => {
    const batchItemFailures = [];
    for (const record of event.Records) {
        try {
```

```
            await processMessageAsync(record, context);
        } catch (error) {
            batchItemFailures.push({ itemIdentifier: record.messageId });
        }
    }
    return { batchItemFailures };
};

async function processMessageAsync(record, context) {
    if (record.body && record.body.includes("error")) {
        throw new Error("There is an error in the SQS Message.");
    }
    console.log(`Processed message: ${record.body}`);
}
```

Signaler les défaillances d'articles par lots SQS avec Lambda à l'aide de TypeScript.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import { SQSEvent, SQSBatchResponse, Context, SQSBatchItemFailure, SQSRecord }
 from 'aws-lambda';

export const handler = async (event: SQSEvent, context: Context):
 Promise<SQSBatchResponse> => {
    const batchItemFailures: SQSBatchItemFailure[] = [];

    for (const record of event.Records) {
        try {
            await processMessageAsync(record);
        } catch (error) {
            batchItemFailures.push({ itemIdentifier: record.messageId });
        }
    }

    return {batchItemFailures: batchItemFailures};
};

async function processMessageAsync(record: SQSRecord): Promise<void> {
    if (record.body && record.body.includes("error")) {
        throw new Error('There is an error in the SQS Message.');
    }
    console.log(`Processed message ${record.body}`);
}
```

PHP

Kit SDK pour PHP

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signalement des échecs d'articles par lots SQS avec Lambda à l'aide de PHP.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
<?php

use Bref\Context\Context;
use Bref\Event\Sqs\SqsEvent;
use Bref\Event\Sqs\SqsHandler;
use Bref\Logger\StderrLogger;

require __DIR__ . '/vendor/autoload.php';

class Handler extends SqsHandler
{
    private StderrLogger $logger;
    public function __construct(StderrLogger $logger)
    {
        $this->logger = $logger;
    }

    /**
     * @throws JsonException
     * @throws \Bref\Event\InvalidLambdaEvent
     */
    public function handleSqs(SqsEvent $event, Context $context): void
    {
        $this->logger->info("Processing SQS records");
        $records = $event->getRecords();
```

```
        foreach ($records as $record) {
            try {
                // Assuming the SQS message is in JSON format
                $message = json_decode($record->getBody(), true);
                $this->logger->info(json_encode($message));
                // TODO: Implement your custom processing logic here
            } catch (Exception $e) {
                $this->logger->error($e->getMessage());
                // failed processing the record
                $this->markAsFailed($record);
            }
        }
        $totalRecords = count($records);
        $this->logger->info("Successfully processed $totalRecords SQS records");
    }
}

$logger = new StderrLogger();
return new Handler($logger);
```

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signalement des échecs d'articles par lots SQS avec Lambda à l'aide de Python.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0

def lambda_handler(event, context):
    if event:
        batch_item_failures = []
        sqs_batch_response = {}

        for record in event["Records"]:
```

```
            try:
                print(f"Processed message: {record['body']}")
            except Exception as e:
                batch_item_failures.append({"itemIdentifier":
 record['messageId']})

        sqs_batch_response["batchItemFailures"] = batch_item_failures
        return sqs_batch_response
```

Ruby

Kit SDK pour Ruby

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signalement des échecs d'articles par lots SQS avec Lambda à l'aide de Ruby.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
require 'json'

def lambda_handler(event:, context:)
  if event
    batch_item_failures = []
    sqs_batch_response = {}

    event["Records"].each do |record|
      begin
        # process message
      rescue StandardError => e
        batch_item_failures << {"itemIdentifier" => record['messageId']}
      end
    end

    sqs_batch_response["batchItemFailures"] = batch_item_failures
    return sqs_batch_response
  end
end
```

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples sans serveur.

Signalement des échecs d'articles par lots SQS avec Lambda à l'aide de Rust.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
use aws_lambda_events::{
    event::sqs::{SqsBatchResponse, SqsEvent},
    sqs::{BatchItemFailure, SqsMessage},
};
use lambda_runtime::{run, service_fn, Error, LambdaEvent};

async fn process_record(_: &SqsMessage) -> Result<(), Error> {
    Err(Error::from("Error processing message"))
}

async fn function_handler(event: LambdaEvent<SqsEvent>) ->
 Result<SqsBatchResponse, Error> {
    let mut batch_item_failures = Vec::new();
    for record in event.payload.records {
        match process_record(&record).await {
            Ok(_) => (),
            Err(_) => batch_item_failures.push(BatchItemFailure {
                item_identifier: record.message_id.unwrap(),
            }),
        }
    }

    Ok(SqsBatchResponse {
        batch_item_failures,
    })
}
```

```
#[tokio::main]
async fn main() -> Result<(), Error> {
    run(service_fn(function_handler)).await
}
```

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

AWS contributions de la communauté pour Lambda

AWS contributions communautaires sont des exemples qui ont été créés et sont gérés par plusieurs équipes à travers AWS. Pour faire un commentaire, utilisez le mécanisme fourni dans les référentiels liés.

Exemples

- Création et test d'une application sans serveur

Création et test d'une application sans serveur

Les exemples de code suivants montrent comment créer et tester une application sans serveur à l'aide d'API Gateway avec Lambda et DynamoDB.

.NET

SDK pour .NET

Illustre comment créer et tester une application sans serveur composée d'une API Gateway avec Lambda et DynamoDB à l'aide du kit SDK .NET.

Pour le code source complet et les instructions de configuration et d'exécution, consultez l'exemple complet sur GitHub.

Les services utilisés dans cet exemple

- API Gateway
- DynamoDB

- Lambda

Go

Kit SDK pour Go V2

Illustre comment créer et tester une application sans serveur composée d'une API Gateway avec Lambda et DynamoDB à l'aide du kit SDK Go.

Pour le code source complet et les instructions de configuration et d'exécution, consultez l'exemple complet sur GitHub.

Les services utilisés dans cet exemple

- API Gateway
- DynamoDB
- Lambda

Java

SDK pour Java 2.x

Illustre comment créer et tester une application sans serveur composée d'une API Gateway avec Lambda et DynamoDB à l'aide du kit SDK Java.

Pour le code source complet et les instructions de configuration et d'exécution, consultez l'exemple complet sur GitHub.

Les services utilisés dans cet exemple

- API Gateway
- DynamoDB
- Lambda

Rust

SDK pour Rust

Illustre comment créer et tester une application sans serveur composée d'une API Gateway avec Lambda et DynamoDB à l'aide du kit SDK Rust.

Pour le code source complet et les instructions de configuration et d'exécution, consultez l'exemple complet sur GitHub.

Les services utilisés dans cet exemple

- API Gateway
- DynamoDB
- Lambda

Pour une liste complète des AWS Guides du développeur du SDK et exemples de code, voir Utilisation de Lambda avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

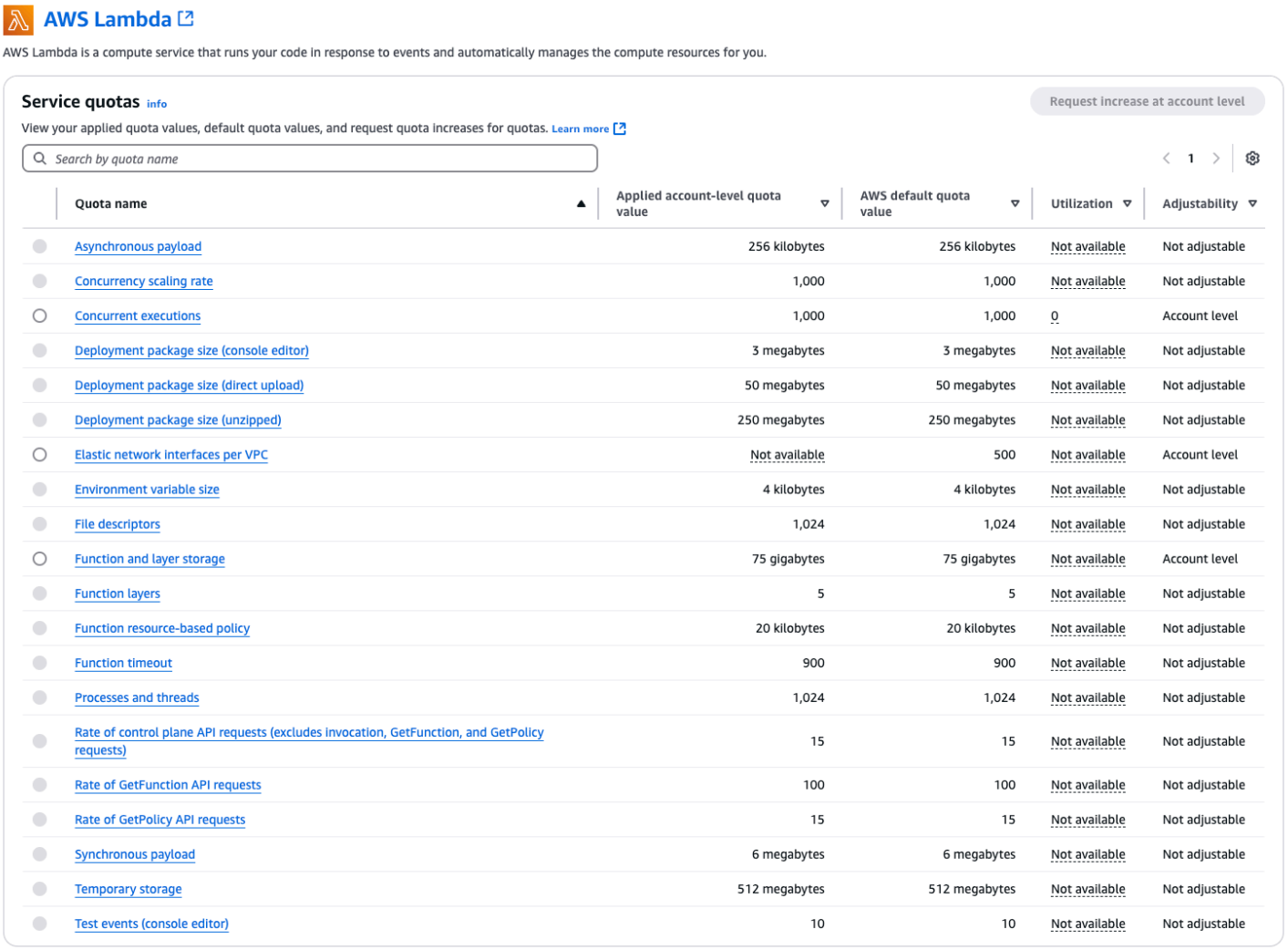
Quotas Lambda

> **Important**
>
> Nouveau Comptes AWS ont réduit les quotas de simultanéité et de mémoire pour les fonctions Lambda et les microVM Lambda, et ont réduit les quotas de processeur virtuel et de taux de demande pour les fonctions Web Lambda. AWS augmente automatiquement ces quotas en fonction de votre utilisation.

AWS Lambda est conçu pour évoluer rapidement afin de répondre à la demande, permettant à vos fonctions d'évoluer pour répondre au trafic de votre application. Lambda est conçu pour les tâches de calcul de courte durée qui ne conservent pas ou ne dépendent pas de l'état entre les invocations. Le code peut être exécuté pendant 15 minutes au maximum en une seule invocation (jusqu'à 90 minutes pour les fonctions Lambda Managed Instances invoquées de manière asynchrone ou via n'importe quel mappage de source d'événements à l'exception d'Amazon MQ et Amazon DocumentDB) et une seule fonction peut utiliser jusqu'à 10 240 Mo de mémoire.

Il est important de comprendre les barrières mises en place pour protéger votre compte et la charge de travail des autres clients. Des quotas de service existent dans tous AWS services et se composent de limites strictes, que vous ne pouvez pas modifier, et de limites souples, pour lesquelles vous pouvez demander des augmentations. Par défaut, tous les nouveaux comptes se voient attribuer un profil de quota qui permet d'explorer AWS services.

Pour voir les quotas qui s'appliquent à votre compte, accédez au tableau de bord Service Quotas. Ici, vous pouvez consulter vos quotas de service, demander une augmentation de quota et consulter l'utilisation actuelle. À partir de là, vous pouvez accéder à un AWS service, tel que Lambda :



AWS Lambda

AWS Lambda is a compute service that runs your code in response to events and automatically manages the compute resources for you.

Service quotas info

View your applied quota values, default quota values, and request quota increases for quotas. Learn more

Request increase at account level

Search by quota name

1

Quota name	Applied account-level quota value	AWS default quota value	Utilization	Adjustability
Asynchronous payload	256 kilobytes	256 kilobytes	Not available	Not adjustable
Concurrency scaling rate	1,000	1,000	Not available	Not adjustable
Concurrent executions	1,000	1,000	0	Account level
Deployment package size (console editor)	3 megabytes	3 megabytes	Not available	Not adjustable
Deployment package size (direct upload)	50 megabytes	50 megabytes	Not available	Not adjustable
Deployment package size (unzipped)	250 megabytes	250 megabytes	Not available	Not adjustable
Elastic network interfaces per VPC	Not available	500	Not available	Account level
Environment variable size	4 kilobytes	4 kilobytes	Not available	Not adjustable
File descriptors	1,024	1,024	Not available	Not adjustable
Function and layer storage	75 gigabytes	75 gigabytes	Not available	Account level
Function layers	5	5	Not available	Not adjustable
Function resource-based policy	20 kilobytes	20 kilobytes	Not available	Not adjustable
Function timeout	900	900	Not available	Not adjustable
Processes and threads	1,024	1,024	Not available	Not adjustable
Rate of control plane API requests (excludes invocation, GetFunction, and GetPolicy requests)	15	15	Not available	Not adjustable
Rate of GetFunction API requests	100	100	Not available	Not adjustable
Rate of GetPolicy API requests	15	15	Not available	Not adjustable
Synchronous payload	6 megabytes	6 megabytes	Not available	Not adjustable
Temporary storage	512 megabytes	512 megabytes	Not available	Not adjustable
Test events (console editor)	10	10	Not available	Not adjustable

Les sections suivantes répertorient les quotas et limites par défaut dans Lambda par catégorie.

Rubriques

- calcul et stockage
- Configuration, déploiement et exécution de fonction
- Requêtes d’API Lambda
- Fonctions durables
- MicroVM Lambda
- Fonctions Web Lambda
- Autres services

calcul et stockage

Lambda définit des quotas pour les ressources de calcul et de stockage que vous pouvez utiliser afin d'exécuter et de stocker des fonctions. Les quotas d'exécutions simultanées et de stockage s'appliquent par Région AWS. Les quotas d'Interface réseau Elastic (ENI) s'appliquent par cloud privé virtuel (VPC), quelle que soit la Région. Les quotas suivants peuvent être augmentés par rapport à leurs valeurs par défaut. Pour de plus amples informations, veuillez consulter Demande d'augmentation de quota dans le Guide de l'utilisateur Service Quotas.

Ressource	Quota par défaut	Peut être augmentée jusqu'à
Exécutions simultanées	1 000	Dizaines de milliers
Stockage des fonctions téléchargées (archives de fichiers .zip) et des couches à l'aide de Lambda-managed rangement. Chaque version de fonction et de couche consomme de l'espace de stockage. Pour éviter les limites de stockage, vous pouvez configurer les fonctions et les couches à utiliser stockage de code S3 autogéré au lieu de cela. Pour respecter les bonnes pratiques en matière d'administration du stockage du code, veuillez consulter Surveillance du stockage de code Lambda dans Serverless Land.	300 Go (décompressé)	Non augmentable. Utiliser stockage de code S3 autogéré pour un stockage au-delà de cette limite.
Stockage des fonctions définies en tant qu'images de conteneur. Ces images sont stockées dans Amazon ECR.	Consultez Service Quotas Amazon ECR.	
Interfaces réseau Elastic par cloud privé virtuel (VPC)	3 000	Milliers

Ressource	Quota par défaut	Peut être augmentée jusqu'à
Note Ce quota est partagé avec d'autres services, tels qu'Amazon Elastic File System (Amazon EFS). Consultez Quotas Amazon VPC.		

Pour en savoir plus sur la simultanéité et la manière dont Lambda met à l'échelle la simultanéité de votre fonction en réponse au trafic, consultez Comprendre le dimensionnement des fonctions d'événement Lambda.

Configuration, déploiement et exécution de fonction

Les quotas suivants s'appliquent à la configuration, au déploiement et à l'exécution des fonctions. Sauf indication contraire, ils ne peuvent pas être modifiés.

Note

La documentation Lambda, les messages de journal et la console utilisent l'abréviation Mo (plutôt que Mio) pour faire référence à 1024 Ko.

Ressource	Quota
Allocation de mémoire des fonctions	128 Mo à 10 240 Mo, par incréments de 1 Mo Remarque : Lambda alloue de la puissance d'UC en fonction de la quantité de mémoire configurée. Vous pouvez augmenter ou réduire la mémoire et la puissance d'UC

Ressource	Quota
	allouées à votre fonction à l'aide du paramètre Mémoire (Mo). À 1 769 Mo, une fonction possède l'équival ent d'un vCPU.
Délai d'expiration des fonctions	900 secondes (15 minutes). Pour les fonctions utilisant AWS Lambda Les instances gérées, les appels asynchrones et les appels de mappage de sources d'événeme nts (sauf Amazon MQ et Amazon DocumentDB) prennent en charge une valeur maximale autorisée de 5 400 secondes (90 minutes).
Variables d'environnement des fonctions	4 Ko, pour toutes les variables d'environnement associées à la fonction, au total
stratégie de fonction basée sur les ressources	20 Ko
Couches de fonctions	5 couches
Limite d'échelle de simultanéité des fonctions	Pour chaque fonction, 1 000 environnements d'exécution toutes les 10 secondes

Ressource	Quota
Charge utile d'invocation (demande et réponse)	6 Mo chacun pour la demande et la réponse (synchrone) 200 Mo pour chaque réponse en streaming (synchrone) 1 Mo (asynchrone) 1 Mo pour la taille totale combinée des valeurs de ligne de requête et d'en-tête
Bande passante pour les réponses diffusées	Non plafonné pour les 6 premiers Mo de la réponse de votre fonction Pour les réponses supérieures à 6 Mo, 2 Mbit/s pour le reste de la réponse
Bande passante réseau par environnement d'exécution	625 Mbit/s. Pour les fonctions qui ne sont pas rattachées à un VPC, vous pouvez demander une augmentation via Console de quotas de service. Après approbation, la bande passante réseau évolue proportionnellement à la mémoire, commençant à 2 048 Mo de mémoire et atteignant un maximum de 3 000 Mbit/s à 10 240 Mo.

Ressource	Quota
Taille du package de déploiement (archive de fichiers .zip)	50 Mo (compressés, lors du chargement via l'API Lambda ou les SDK). Chargez vos fichiers sur Amazon S3. 50 Mo (en cas de chargement via la console Lambda) 250 Mo La taille maximale du contenu d'un package de déploiement, y compris les couches et les environnements d'exécution personnalisés. (décompressé)
Taille des paramètres de l'image de conteneur	16 Ko
Taille du package du code de l'image de conteneur	10 Go (taille maximale de l'image non compressée, comprenant toutes les couches)
Événements de test (éditeur de console)	10
Stockage dans le répertoire `/tmp`	Entre 512 Mo et 10 240 Mo par incréments de 1 Mo

Ressource	Quota
Descripteurs de fichier	1,024 **Note** Les instances gérées Lambda utilisent une limite de descripteurs de fichier plus élevée de 4 096. Pour plus d'informations, consultez Comprendre l'environnement d'exécution des instances gérées Lambda.
Exécution processes/threads	1,024 **Note** Les instances gérées Lambda utilisent les limites de processus et de thread par défaut de Fusée à bouteilles. Pour plus d'informations, consultez Comprendre l'environnement d'exécution des instances gérées Lambda.

Requêtes d'API Lambda

Les quotas suivants sont associés aux demandes d'API Lambda.

Ressource	Quota
Demandes d’invocation par fonction par région (synchrone)	Chaque instance de votre environnement d’exécution peut servir jusqu’à 10 demandes par seconde. En d’autres termes, la limite d’invocation totale correspond à 10 fois votre limite de simultanéité. Consultez Comprendre le dimensionnement des fonctions d'événement Lambda.
Demandes d’invocation par fonction par région (asynchrone)	Chaque instance de votre environnement d’exécution peut servir un nombre illimité de demandes. En d’autres termes, la limite d’invocation totale est basée uniquement sur la simultanéité disponible pour votre fonction. Consultez Comprendre le dimensionnement des fonctions d'événement Lambda.
Demandes d’invocation par version ou alias de fonction (demandes par seconde)	10 x simultanéité provisionnée **Note** Ce quota s’applique uniquement aux fonctions qui utilisent la simultanéité provisionnée.
Demandes d'API GetFunction	100 requêtes par seconde. Il ne peut pas être augmenté.
Demandes d'API GetPolicy	15 requêtes par seconde. Il ne peut pas être augmenté.

Ressource	Quota
Le reste des demandes d'API du plan de contrôle (à l'exclusion de l'invocation, GetFunction, et GetPolicy demandes)	15 requêtes par seconde pour l'ensemble des API (et non 15 requêtes par seconde par API). Il ne peut pas être augmenté.

Fonctions durables

Les quotas suivants s'appliquent à fonctions durables. Des quotas s'appliquent par Région AWS. Des valeurs par défaut plus élevées s'appliquent aux États-Unis de l'Est (Virginie du Nord), à l'Ouest des États-Unis (Oregon) et à l'Europe (Irlande), comme indiqué dans le tableau. Sauf indication contraire, ces quotas peuvent être augmentés. Pour de plus amples informations, veuillez consulter Demande d'augmentation de quota dans le Guide de l'utilisateur Service Quotas.

Ressource	Quota par défaut
Exécutions durables et à fonctionnement maximal	5 000 000 par région. 10 000 000 dans l'est des États-Unis (Virginie du Nord), l'ouest des États-Unis (Oregon) et l'Europe (Irlande). Il s'agit d'une limite souple qui peut être augmentée.
Nombre maximum d'opérations durables par exécution durable	30 000 Il ne peut pas être augmenté. Pour plus d'informations, voir Opérations durables disponibles.
Stockage d'exécution durable écrit en mégaoctets	100 Mo Il ne peut pas être augmenté. La taille cumulée de la charge utile est maintenue par des fonctions durables par exécution. Pour plus d'informa

Ressource	Quota par défaut
	tions, voir données persistantes par opération durable.
Taille de charge utile maximale par opération durable	1 Mo Il ne peut pas être augmenté. S'applique aux charges utiles des points de contrôle et des rappels.
Taux d'invocation des fonctions pour lancer des exécutions durables	3 000 requêtes par seconde. 6 000 demandes par seconde dans l'est des États-Unis (Virginie du Nord), l'ouest des États-Unis (Oregon) et l'Europe (Irlande).
Demandes d'API CheckpointDurableExecution	10 000 requêtes par seconde. 20 000 demandes par seconde dans l'est des États-Unis (Virginie du Nord), l'ouest des États-Unis (Oregon) et l'Europe (Irlande).
Demandes d'API GetDurableExecution	30 requêtes par seconde.
Demandes d'API GetDurableExecutionHistory	15 requêtes par seconde.
Demandes d'API GetDurableExecutionState	10 000 requêtes par seconde. 20 000 demandes par seconde dans l'est des États-Unis (Virginie du Nord), l'ouest des États-Unis (Oregon) et l'Europe (Irlande).
Demandes d'API ListDurableExecutionsByFunction	15 requêtes par seconde.

Ressource	Quota par défaut
Demandes d'API SendDurableExecutionCallbackFailure	3 000 requêtes par seconde. 6 000 demandes par seconde dans l'est des États-Unis (Virginie du Nord), l'ouest des États-Unis (Oregon) et l'Europe (Irlande).
Demandes d'API SendDurableExecutionCallbackHeartbeat	3 000 requêtes par seconde. 6 000 demandes par seconde dans l'est des États-Unis (Virginie du Nord), l'ouest des États-Unis (Oregon) et l'Europe (Irlande).
Demandes d'API SendDurableExecutionCallbackSuccess	3 000 requêtes par seconde. 6 000 demandes par seconde dans l'est des États-Unis (Virginie du Nord), l'ouest des États-Unis (Oregon) et l'Europe (Irlande).
Demandes d'API StopDurableExecution	300 requêtes par seconde. 600 demandes par seconde dans l'est des États-Unis (Virginie du Nord), l'ouest des États-Unis (Oregon) et l'Europe (Irlande).

MicroVM Lambda

Lambda MicroVMS définit des quotas pour les requêtes de calcul, de stockage et d'API. Les quotas marqués comme ajustables peuvent être augmentés via la console Service Quotas.

> **Note**
>
> Les microVM Lambda prennent en charge l'ARM64 (AWS Architecture (graviton).

calcul et stockage

Ressource	Quota par défaut	Ajustable
Mémoire allouée à toutes les micromachines virtuelles (par compte, par région)	400 Go (soit 200 micromachines virtuelles avec 2 Go de mémoire configuré e chacune ou 400 micromachines virtuelles avec 1 Go de mémoire configuré e chacune). 1 024 Go dans l'est des États-Unis (Virginie du Nord), l'ouest des États-Uni s (Oregon), l'est des États-Unis (Ohio) et la région Asie-Pacifique (Tokyo) (soit 512 micromach ines virtuelles avec 2 Go de mémoire configurée chacune ou 1 024 micromach ines virtuelles avec 1 Go de mémoire configurée chacune). Explosible jusqu'à quatre fois ce quota.	Oui
Durée d'exécution maximale par microVM	8 heures (28 800 secondes)	Non

Images et versions

Ressource	Quota par défaut	Ajustable
Images MicroVM par compte et par région	100	Oui
Versions par image MicroVM	50	Oui
Création simultanée d'images (par compte, par région)	5 10 dans l'est des États-Unis (Virginie du Nord), l'ouest des États-Unis (Oregon), l'est des États-Unis (Ohio) et l'Asie-Pacifique (Tokyo)	Oui

Per-MicroVM débit

Ressource	Limite	Ajustable
Connexions simultanées par microVM	8 (1 processeur virtuel), 16 (2 processeurs virtuels), 32 (4 processeurs virtuels), 64 (8 processeurs virtuels), 128 (16 processeurs virtuels)	Non
Demandes par seconde par microVM	40 (4 processeurs virtuels/8 Go), 160 (16 processeurs virtuels/32 Go)	Non

limites de débit d'API

Opération API	Taux (TPS)	Mode rafale	Ajustable
`RunMicrovm`	5	5	Oui
`ResumeMicrovm`	5	5	Oui
`SuspendMicrovm`	2	2	Oui
`TerminateMicrovm`	10	10	Oui
`GetMicrovm`	100	100	Oui
`CreateMicrovmAuthToken`	50	50	Oui
`CreateMicrovmShell AuthToken`	5	5	Oui

> **Note**
>
> TPS = transactions par seconde. Ces limites tarifaires s'appliquent par compte et par région. Réessayez les requêtes limitées en utilisant un backoff exponentiel avec gigue.

Fonctions Web Lambda

Avec AWS Lambda Web Functions, vous exécutez des applications Web et des backends d'API en tant que serveurs HTTP sans serveur. Les quotas sont les valeurs maximales pour les ressources et les paramètres des fonctions Web. Les exemples incluent le nombre de points de terminaison par fonction Web, la mémoire d'un environnement d'exécution et les demandes par seconde pour votre compte. Les connaître avant le déploiement vous permet de concevoir votre application et de dimensionner ses paramètres de dimensionnement des terminaux en fonction de ses besoins. La plupart des quotas ont des valeurs par défaut qui fonctionnent pour des charges de travail classiques et ne peuvent pas être modifiées. Vous pouvez demander une augmentation des quotas de compte ajustables, qui peuvent varier d'un compte à l'autre.

Les quotas relatifs aux fonctions Web s'appliquent dans les domaines suivants :

- Par fonction Web — Points finaux et révisions.
- Par point de terminaison — Environnements maximaux, limite de débit et nombre de révisions partageant le trafic.
- Par révision — Taille du package de déploiement, taille de la variable d'environnement et délai d'expiration de la demande.
- Par environnement d'exécution — vCPU, mémoire, requêtes simultanées, `/tmp` taille du répertoire, descripteurs de fichiers, processus et threads et délai d'initialisation.
- Par demande — Taille de l'en-tête de la demande.
- Par compte, dans chaque Région AWS — Demandes par seconde et vCPU Arm64.

> **Note**
>
> Pour voir les valeurs de quota de compte qui s'appliquent à votre compte dans une région, appelez `GetWebAccountSettings`. Pour suivre l'utilisation par rapport à ces quotas, voir the section called “Indicateurs régionaux d'utilisation et de limitation”.

Quotas relatifs aux fonctions Web, à la révision et à l'environnement d'exécution

Le tableau suivant répertorie les quotas pour chaque fonction Web, chaque révision, chaque environnement d'exécution et chaque demande.

Ressource	Quota par défaut	Ajustable
Points de terminaison par fonction Web	10	Non
Révisions par fonction Web	50 (cible de nettoyage automatique). Le nombre peut temporairement dépasser 50. Consultez the section called “Limites de	Non

Ressource	Quota par défaut	Ajustable
	révision et nettoyage automatique”.	
Taille du package de déploiement	512 Mo (décompressé)	Non
Taille de la variable d'environnement	32 Ko	Non
Taille de l'en-tête de la demande	128 Ko	Non
`/tmp` taille du répertoire	512 Mo	Non
vCPU par environnement d'exécution	2	Non
Mémoire par environnement d'exécution	2 Go	Non
Demandes simultanées par environnement (`maxConcurrencyPerEnvironment`)	64 (plage 1 à 128). Consultez the section called “Limite de simultanéité dynamique par environnement”.	Non
Délai d'expiration de la demande	30 secondes (plage de 3 à 900)	Non
Délai d'initialisation (temps nécessaire pour que votre serveur commence à écouter)	10 secondes	Non
Descripteurs de fichiers par environnement d'exécution	1,024	Non
Processus et threads par environnement d'exécution	1,024	Non

Quotas de points de terminaison

Le tableau suivant répertorie les quotas de terminaux.

Ressource	Quota par défaut	Ajustable
Nombre maximal d'environnements par terminal (`scalingConfig.maxEnvironments`)	Facultatif. Non défini par défaut. Valeurs valides : 2 à 10 000. Appliqué dans chaque région. Le quota de processeurs virtuels du compte peut limiter le point de terminaison à un nombre réduit d'environnements d'exécution.	Non
Limite de débit par point final (`throttleConfig.rateLimit`)	Facultatif. Non défini par défaut. Les valeurs valides sont 0, 100 à 1 000 par pas de 100 et 2 000 à 10 000 par pas de 1 000 demandes par seconde. Lambda applique cette limite séparément dans chaque région. La valeur 0 bloque tout le trafic. Lorsqu'il n'est pas défini, le quota par terminal de 10 000 demandes par seconde s'applique.	Non
Révisions maximales par paramètre (poids des révisions)	2	Non
Fourchette de poids de révision	1–100	Non

Quotas de comptes

Le tableau suivant répertorie les quotas de comptes qui s'appliquent à chaque compte. Région AWS.

Ressource	Quota par défaut	Ajustable
Demandes par seconde et par compte	100 000	Oui
vCPU Arm64 pour les environnements d'exécution, par compte, par région	2 000. Chaque environnement d'exécution utilise 2 processeurs virtuels.	Oui

Contraintes du réseau

Les contraintes suivantes s'appliquent à la mise en réseau des fonctions Web.

Élément	Contrainte
Connecteurs réseau de sortie par révision	0 ou 1
Référence de connecteur	Version-qualified ARN
Compte Connector et région	Identique à la fonction Web
Type de ressource de calcul du connecteur	Exactement un ; utilisez `WebFunction`
Modifier le connecteur d'une révision	Créer une nouvelle révision
Révisions acheminées par un seul point de terminaison	1 ou 2
Types de terminaux prenant en charge les connecteurs réseau de sortie	`HomeRegion` uniquement
Déploiement automatique	`LatestRevision` ou `Disabled` pour `HomeRegion` ; `Disabled` uniquement pour `MultiRegion` et `PerRegion`

Élément	Contrainte
Type de point de terminaison et ensemble de régions	Corrigé lors de la création du terminal
Accès public direct	`IPv4` uniquement
Accès privé aux terminaux avec AWS PrivateLink	Non disponible

Autres services

Quotas pour d'autres services, tels que Gestion des identités et des accès AWS (IAM), Amazon CloudFront (Lambda @Edge) et Amazon Virtual Private Cloud (Amazon VPC) peuvent avoir un impact sur vos fonctions Lambda. Pour plus d'informations, consultez Quotas Service AWS dans le Référence générale d'Amazon Web Services et Invoquer Lambda avec des événements provenant d'autres AWS services.

De nombreuses applications impliquant Lambda utilisent plusieurs AWS services. Étant donné que les différents services ont des quotas différents pour différentes fonctionnalités, il peut être difficile de gérer ces quotas dans l'ensemble de votre application. API Gateway a une limitation par défaut de 10 000 requêtes par seconde, alors que Lambda a une limitation par défaut de 1 000. En raison de cette incompatibilité, il est possible que Lambda puisse gérer davantage de demandes entrantes provenant d'API Gateway. Ce problème peut être résolu en demandant que la limite de simultanéité de Lambda soit augmentée afin qu'elle corresponde au niveau de trafic attendu.

Les tests de charge de votre application vous permettent de surveiller ses performances de bout en bout avant de la déployer en production. Lors d'un test de charge, vous pouvez identifier les quotas susceptibles de limiter les niveaux de trafic que vous attendez et prendre les mesures nécessaires en conséquence.

Historique du document

Le tableau suivant décrit les modifications importantes apportées au Guide du développeur d'AWS Lambda après mai 2018. Pour recevoir les notifications des mises à jour de cette documentation, abonnez-vous au flux RSS.

Modification	Description	Date
AWS mise à jour des politiques gérées	Lambda a ajouté une nouvelle politique AWS gérée (`AWSLambdaNetworkConnectorOperatorPolicy`) pour accorder des autorisations pour créer et administrer des ressources d'interface réseau élastique (ENI) gérées par le Lambda Network Connector. Pour plus d'informations, consultez la section Mises à jour Lambda des politiques AWS gérées.	19 juin 2026
AWS mise à jour des politiques gérées	Lambda a mis à jour la politique `AWSLambdaManagedEC2ResourceOperator` gérée pour ajouter CloudWatch des autorisations Amazon (`logs:CreateLogGroup`, `logs:CreateLogStream`, `logs:PutLogEvents`). Pour plus de détails, consultez la section Mises à jour Lambda des politiques AWS gérées.	10 juin 2026

Self-managed Stockage de code S3	Lambda prend désormais en charge les compartiments S3 autogérés pour le stockage des codes de fonction et de couche. Vous pouvez configurer Lambda pour référencer votre code directement depuis votre compartiment S3, éliminant ainsi les limites Lambda-managed de stockage. Pour plus de détails, consultez la section Stockage de code Self-managed S3.	30 avril 2026
AWS mise à jour des politiques gérées	Lambda a mis à jour la politique `AWSLambdaManagedEC2ResourceOperator` gérée pour ajouter l'`ec2:DescribeVpcEncryptionControls` autorisation. Pour plus de détails, consultez la section Mises à jour Lambda des politiques AWS gérées.	23 avril 2026
AWS mises à jour des politiques gérées	Lambda a publié une nouvelle politique gérée `AWSLambdaBasicDurableExecutionRolePolicy` qui fournit des autorisations d'écriture sur les CloudWatch journaux et des read/write autorisations sur les API d'exécution durables utilisées par les fonctions durables Lambda.	1er décembre 2025

Service-linked rôle pour Lambda	Lambda prend désormais en charge un rôle lié à un service (`AWSServiceRoleForLambda`) qui permet à Lambda de mettre fin aux instances gérées dans le cadre des fournisseurs de capacité Lambda.	30 novembre 2025
Instances gérées Lambda	Lambda prend désormais en charge les instances gérées, qui fournissent une capacité de calcul dédiée à vos fonctions avec des performances, une sécurité et un contrôle améliorés. Pour plus de détails, consultez Instances gérées Lambda.	30 novembre 2025
AWS mises à jour des politiques gérées	Lambda a ajouté une nouvelle politique AWS gérée (`AWSLambdaBasicDurableExecutionRolePolicy`).	30 novembre 2025
AWS mises à jour des politiques gérées	Lambda a mis à jour la politique AWS gérée existante `AWSLambda_FullAccess`), autorise les `iam:CreateServiceLinkedRole` actions `kms:DescribeKey` et.	30 novembre 2025

AWS mise à jour des politiques gérées	Lambda a ajouté une nouvelle politique AWS gérée (`AWSLambdaManagedEC2ResourceOperator`) pour permettre la gestion automatisée des instances Amazon EC2 pour les fournisseurs de capacité Lambda. Pour plus de détails, consultez la section Mises à jour Lambda des politiques AWS gérées.	30 novembre 2025
AWS mise à jour des politiques gérées	Lambda a ajouté une nouvelle politique AWS gérée (`AWSLambdaServiceRolePolicy`). Pour plus de détails, consultez la section Mises à jour Lambda des politiques AWS gérées.	30 novembre 2025
AWS mises à jour des politiques gérées	Lambda a mis à jour deux politiques AWS gérées existantes (`AWSLambda_ReadOnlyAccess` et`AWSLambda_FullAccess`).	20 février 2025
Node.js Temps d'exécution 22.x	Lambda prend désormais en charge Node.js 22 en tant qu'environnement d'exécution géré et image de base de conteneur (`nodejs22.x`).	22 novembre 2024

SnapStart support pour Python et .NET	Lambda SnapStart est désormais disponible pour les environnements d'exécution gérés par Python et .NET, en commençant `python3.12` par et. `dotnet8`	18 novembre 2024
Environnement d'exécution Python 3.13	Lambda prend désormais en charge Python 3.13 en tant qu'environnement d'exécuti on géré et image de base de conteneur.	13 novembre 2024
Chiffrement géré par le client pour les packages de déploiement .zip	Lambda prend désormais en charge AWS KMS le chiffrement par clé géré par le client pour les packages de déploiement .zip.	8 novembre 2024
Assistance SnapStart dans les nouvelles régions	Lambda SnapStart est désormais disponible dans les régions suivantes : Europe (Espagne), Europe (Zurich), Asie-Pacifique (Melbourne), Asie-Pacifique (Hyderabad) et Moyen-Orient (Émirats arabes unis).	12 janvier 2024
AWS mises à jour des politiques gérées	Lambda a mis à jour une politique AWS gérée existante (`AWSLambdaVPCAccess ExecutionRole`).	5 janvier 2024

Exécution Python 3.12	Lambda prend désormais en charge Python 3.12 en tant qu'exécution managée et image de base de conteneur . Pour plus d'informations, consultez le runtime Python 3.12 désormais disponible AWS Lambda sur le blog AWS Compute.	14 décembre 2023
Environnement d'exécution Java 21	Lambda prend désormais en charge Java 21 en tant qu'exécution managée et image de base de conteneur (`java21`).	16 novembre 2023
Node.js Temps d'exécution 20.x	Lambda prend désormais en charge Node.js 20 en tant qu'environnement d'exécuti on géré et image de base de conteneur (`nodejs20.x`)). Pour plus d'informations, consultez le runtime Node.js 20.x désormais disponible AWS Lambda sur le blog AWS Compute.	14 novembre 2023
Exécution provided.al2023	Lambda prend désormais en charge Amazon Linux 2023 en tant qu'environnement d'exécution géré et image de base de conteneur. Pour plus d'informations, consultez Présentation de l'environ nement d'exécution Amazon Linux 2023 pour AWS Lambda sur le blog AWS Compute.	9 novembre 2023

Prise en charge d'IPv6 pour les sous-réseaux à double pile	Lambda prend désormais en charge le trafic IPv6 sortant vers les sous-réseaux à double pile. Pour plus d'informations, consultez la section Prise en charge d'IPv6.	12 octobre 2023
Test de fonctions et d'applications sans serveur	Découvrez les techniques de débogage et d'automatisation des tests des fonctions sans serveur dans le cloud. Un chapitre sur les tests et des ressources sont désormais inclus dans les sections consacrées aux langages Python et Typescript. Pour en savoir plus, veuillez consulter la rubrique Tester des fonctions et des applications sans serveur.	16 juin 2023
Exécution Ruby 3.2	Lambda prend désormais en charge une nouvelle exécution pour Ruby 3.2. Pour plus d'informations, veuillez consulter la rubrique Création de fonctions Lambda avec Ruby.	7 juin 2023

Streaming des réponses	Lambda prend désormais en charge le streaming des réponses des fonctions. Pour plus d'informations, consultez Configuration d'une fonction Lambda pour le streaming des réponses (français non garanti).	6 avril 2023
Métriques d'invocations asynchrones	Lambda publie des métriques d'invocations asynchrones. Pour plus d'informations, consultez Métriques d'invocations asynchrones.	9 février 2023
Contrôles de version de l'environnement d'exécution	Lambda publie de nouvelles versions de l'environnement d'exécution qui incluent des mises à jour de sécurité, des corrections de bogues et de nouvelles fonctions . Vous pouvez désormais contrôler quand vos fonctions sont mises à jour vers les nouvelles versions de l'environnement d'exécution. Pour plus d'informations, consultez Mises à jour de l'environnement d'exécution Lambda (français non garanti).	23 janvier 2023

Lambda SnapStart	Utilisez Lambda SnapStart pour réduire le temps de démarrage des fonctions Java sans provisionner de ressources supplémentaires ni implémenter des optimisations de performances complexes. Pour plus d'informations, consultez la section Améliorer les performances de démarrage avec Lambda SnapStart.	28 novembre 2022
Node.js 18 temps d'exécution	Lambda prend désormais en charge un nouveau runtime pour Node.js 18. Node.js 18 utilise Amazon Linux 2. Pour plus de détails, consultez la section Création de fonctions Lambda avec Node.js.	18 novembre 2022
lambda : clé de SourceFunctionArn condition	Pour une AWS ressource, la clé de `lambda:SourceFunctionArn` condition filtre l'accès à la ressource par l'ARN d'une fonction Lambda. Pour plus d'informations, consultez utilisation des identifiants d'un environnement d'exécution Lambda.	1et juillet 2022

Node.js 16 temps d'exécution	Lambda prend désormais en charge un nouveau runtime pour Node.js 16. Node.js 16 utilise Amazon Linux 2. Pour plus de détails, consultez la section Création de fonctions Lambda avec Node.js.	11 mai 2022
URL de fonctions Lambda	Lambda prend désormais en charge les URL de fonctions , qui sont des points de terminaison HTTP(S) dédiés pour les fonctions Lambda. Pour plus d'informations, consultez URL de fonctions Lambda.	6 avril 2022
Événements de test partagés dans la AWS Lambda console	Lambda prend désormais en charge le partage d'événements de test avec d'autres utilisateurs dans le même Compte AWS. Pour plus de détails, consultez Test des fonctions Lambda dans la console.	16 mars 2022
PrincipalOrgId dans les politiques fondées sur les ressources	Lambda prend désormais en charge l'octroi d'autorisations à une organisation dans AWS Organizations. Pour plus d'informations, consultez Utilisation de stratégies basées sur les ressources pour AWS Lambda.	11 mars 2022

Exécution .NET 6	Lambda prend désormais en charge un nouvel environnement d'exécution pour .NET 6. Pour en savoir plus, consultez Environnements d'exécution Lambda.	23 février 2022
Filtrage des événements pour les sources d'événements Kinesis, DynamoDB et Amazon SQS	Lambda prend désormais en charge le filtrage des événements pour les sources d'événements Kinesis, DynamoDB et Amazon SQS. Pour plus de détails, consultez Filtrage des événements Lambda.	24 novembre 2021
Authentification MTL pour Amazon MSK et sources d'événements Apache Kafka autogérées	Lambda prend désormais en charge l'authentification MTL pour Amazon MSK et les sources d'événements Apache Kafka autogérées. Pour plus de détails, consultez Utilisation de Lambda avec Amazon MSK.	19 novembre 2021
Lambda sur Graviton2	Lambda prend désormais en charge Graviton2 pour les fonctions utilisant l'architecture arm64. Pour plus de détails, consultez Architectures de l'ensemble des instructions Lambda.	29 septembre 2021

Exécution Python 3.9	Lambda prend désormais en charge un nouveau runtime pour Python 3.9. Pour en savoir plus, consultez Environnements d'exécution Lambda.	16 août 2021
Nouvelles versions d'exécution pour Node.js Python et Java	De nouvelles versions d'exécution sont disponibles pour Node.js Python et Java. Pour en savoir plus, consultez Environnements d'exécution Lambda.	21 juillet 2021
Prise en charge de RabbitMQ en tant que source d'événements sur Lambda	Lambda prend désormais en charge Amazon MQ pour RabbitMQ en tant que source d'événements. Amazon MQ est un service d'agent de messages géré pour Apache ActiveMQ, et RabbitMQ, qui facilite la configuration et l'utilisation d'agents de messages dans le cloud. Pour plus de détails, consultez Utilisation de Lambda avec Amazon MQ.	7 juillet 2021

SASL/PLAIN authentification pour Kafka autogéré sur Lambda	SASL/PLAIN est désormais un mécanisme d'authentification pris en charge pour les sources d'événements Kafka autogérées sur Lambda Les clients utilisant SASL/PLAIN déjà leur cluster Kafka autogéré peuvent désormais facilement utiliser Lambda pour créer des applications grand public sans avoir à modifier leur mode d'authentification. Pour plus d'informations, consultez Utilisation de Lambda avec Apache Kafka autogéré.	29 juin 2021
API d'extensions Lambda	Disponibilité générale pour les extensions Lambda. Utilisez des extensions pour augmenter vos fonctions Lambda. Vous pouvez utiliser des extensions fournies par des partenaires Lambda ou créer vos propres extensions Lambda. Pour plus de détails, consultez API Extensions Lambda.	24 mai 2021
Nouvelle expérience de la console Lambda	La console Lambda a été remaniée pour améliorer les performances et la cohérence.	2 mars 2021

Node.js 14 temps d'exécution	Lambda prend désormais en charge un nouveau runtime pour Node.js 14. Node.js 14 utilise Amazon Linux 2. Pour plus de détails, consultez la section Création de fonctions Lambda avec Node.js.	27 janvier 2021
Images de conteneurs Lambda	Lambda prend désormais en charge les fonctions définies en tant qu'images conteneur s. Vous pouvez combiner la flexibilité des outils de conteneur avec l'agilité et la simplicité opérationnelle de Lambda pour générer des applications. Pour plus de détails, consultez Utilisation d'images de conteneurs avec Lambda.	1er décembre 2020

Signature de code pour les fonctions Lambda	Lambda prend désormais en charge la signature de code. Les administrateurs peuvent configurer des fonctions Lambda de façon à n'accepter que du code signé lors du déploiement. Lambda vérifie les signature s afin de s'assurer que le code n'est pas modifié ou altéré. En outre, Lambda s'assure que le code est signé par des développeurs de confiance avant d'accepter le déploiement. Pour plus de détails, consultez Configura tion de la signature de code pour Lambda.	23 novembre 2020
Aperçu : API de journaux d'exécution Lambda	Lambda prend désormais en charge l'API Runtime Logs. Les extensions Lambda peuvent utiliser l'API Logs pour s'abonner à des flux de journaux dans l'environ nement d'exécution. Pour plus de détails, consultez API Runtime Logs Lambda.	12 novembre 2020

Nouvelle source d'événements pour Amazon MQ	Lambda prend désormais en charge Amazon MQ en tant que source d'événements. Utilisez une fonction Lambda pour traiter les enregistr ements de votre agent de messages Amazon MQ. Pour plus de détails, consultez Utilisation de Lambda avec Amazon MQ.	5 novembre 2020
Aperçu : API d'extensions Lambda	Utilisez des extensions Lambda pour augmenter vos fonctions Lambda. Vous pouvez utiliser des extension s fournies par des partenaires Lambda ou créer vos propres extensions Lambda. Pour plus de détails, consultez API Extensions Lambda.	8 octobre 2020
Prise en charge de Java 8 et des environnements d'exécuti on personnalisés sur AL2	Lambda prend désormais en charge Java 8 et les environne ments d'exécution (runtimes) personnalisés sur Amazon Linux 2. Pour en savoir plus, consultez Environnements d'exécution Lambda.	12 août 2020

Nouvelle source d'événements pour Amazon Managed Streaming for Apache Kafka	Lambda prend désormais en charge Amazon MSK en tant que source d'événements. Utilisez une fonction Lambda avec Amazon MSK pour traiter des enregistrements dans une rubrique Kafka. Pour plus de détails, consultez Utilisation de Lambda avec Amazon MSK.	11 août 2020
Clés de condition IAM pour les paramètres du VPC Amazon	Vous pouvez désormais utiliser les clés de Lambda-specific condition pour les paramètres VPC. Par exemple, vous pouvez exiger que toutes les fonctions de votre organisation soient connectées à un VPC. Vous pouvez également spécifier les sous-réseaux et les groupes de sécurité que les utilisateurs de la fonction peuvent et ne peuvent pas utiliser. Pour plus de détails, consultez Configuration du VPC pour les fonctions IAM.	10 août 2020

Paramètres de simultanéité pour les utilisateurs de Kinesis Stream HTTP/2	Vous pouvez désormais utiliser les paramètres de simultanéité suivants pour les utilisateurs de Kinesis avec un fan-out amélioré (HTTP/2 streams) : ParallelizationFactor, MaximumRetryAttempts, MaximumRecordAgeInSeconds et. DestinationConfig BisectBatchOnFunctionError Pour plus de détails, consultez la section Utilisation AWS Lambda avec Amazon Kinesis.	7 juillet 2020
Fenêtre de traitement par lots pour les utilisateurs de Kinesis HTTP/2 Stream	Vous pouvez désormais configurer une fenêtre de traitement par lots (MaximumBatchingWindowInSeconds) pour les HTTP/2 flux. Lambda lit les enregistrements du flux jusqu'à avoir rassemblé un lot complet, ou jusqu'à l'expiration de la fenêtre de traitement par lots. Pour plus de détails, consultez la section Utilisation AWS Lambda avec Amazon Kinesis.	18 juin 2020

Prise en charge des systèmes de fichiers Amazon EFS	Vous pouvez désormais connecter un système de fichiers Amazon EFS à vos fonctions Lambda pour un accès réseau partagé aux fichiers. Pour plus de détails, consultez Configuration de l'accès au système de fichiers pour les fonctions Lambda.	16 juin 2020
AWS CDK exemples d'applications dans la console Lambda	La console Lambda inclut désormais des exemples d'applications qui utilisent le Cloud Development Kit AWS (AWS CDK) for TypeScript. AWS CDK Il s'agit d'un framework qui vous permet de définir les ressources de votre application en Python TypeScript, Java ou .NET.	1 juin 2020
Prise en charge de l'exécution de .NET Core 3.1.0 dans AWS Lambda	AWS Lambda prend désormais en charge le runtime .NET Core 3.1.0. Pour en savoir plus, consultez la page .NET Core CLI.	31 mars 2020

Prise en charge des API HTTP d'API Gateway	Documentation mise à jour et étendue pour l'utilisation de Lambda avec API Gateway, incluant la prise en charge des API HTTP. Ajout d'un exemple d'application qui crée une API et fonctionne avec CloudFormation. Pour plus de détails, consultez Utilisation de Lambda avec Amazon API Gateway.	23 mars 2020
Ruby 2.7	Un nouvel environnement d'exécution est disponible pour Ruby 2.7, ruby2.7, qui est le premier environnement d'exécution Ruby à utiliser Amazon Linux 2. Pour plus d'informations, consultez Création de fonctions Lambda avec Ruby.	19 février 2020

Métriques de simultanéité	Lambda rapporte désormais les métriques `ConcurrentExecutions` pour l'ensemble des fonctions, alias et versions. Vous pouvez afficher un graphique pour cette métrique dans la page de surveillance de votre fonction. Auparavant, `ConcurrentExecutions` était seulement signalé au niveau du compte et pour les fonctions utilisant la simultanéité réservée. Pour plus d'informations, consultez AWS Lambda Métriques des fonctions.	18 février 2020

Mise à jour des états des fonctions	Les états de fonction sont désormais appliqués pour toutes les fonctions par défaut. Lorsque vous connectez une fonction à un VPC, Lambda crée des interfaces réseau Elastic partagées. Cela permet à votre fonction d'évoluer sans créer d'interfaces réseau supplémentaires. Pendant ce temps, vous ne pouvez pas effectuer d'opérations supplémentaires sur la fonction, y compris la mise à jour de sa configuration et de ses versions de publication. Dans certains cas, l'invocation est également affectée. Les détails sur l'état actuel d'une fonction sont disponibles à partir de l'API Lambda. Cette mise à jour est publiée en plusieurs phases. Pour plus de détails, consultez la section Cycle de vie des états Lambda mis à jour pour les réseaux VPC sur le AWS Compute Blog. Pour plus d'informations sur les états, consultez États de fonctions AWS Lambda.	24 janvier 2020

Mises à jour de la sortie de l'API de configuration de fonction	Ajout de codes de raison à StateReasonCode (InvalidSubnet, InvalidSecurityGroup) et LastUpdateStatusReasonCode (SubnetOutOfIPAddresses, InvalidSubnet, InvalidSecurityGroup) pour les fonctions qui se connectent à un VPC. Pour plus d'informations sur les états, consultez États de fonctions AWS Lambda.	20 janvier 2020
Simultanéité allouée	Vous pouvez désormais allouer la simultanéité provisionnée pour une version de fonction ou un alias. La simultanéité provisionnée permet à une fonction d'évoluer sans fluctuations de latence. Pour plus de détails, consultez Gestion de la simultanéité pour une fonction Lambda.	3 décembre 2019

Créer un proxy de base de données	Vous pouvez désormais utiliser la console Lambda pour créer un proxy de base de données pour une fonction Lambda. Un proxy de base de données permet à une fonction d'atteindre des niveaux de simultanéité élevés sans épuiser les connexion s de base de données. Pour plus de détails, consultez Configuration de l'accès à une base de données pour une fonction Lambda.	3 décembre 2019
Prise en charge des percentil es pour la métrique de durée	Vous pouvez désormais filtrer la métrique de durée en fonction des percentiles. Pour plus d'informations, consultez Métriques AWS Lambda.	26 novembre 2019
Augmentation de la simultané ité pour des sources d'événement de flux	Une nouvelle option pour les mappages de source d'événements de flux DynamoDB et de flux Kinesis vous permet de traiter plusieurs lots à la fois à partir de chaque partition. Lorsque vous augmentez le nombre de lots simultanés par partition , la simultanéité de votre fonction peut atteindre dix fois le nombre de partitions dans votre flux. Pour en savoir plus, consultez Mappage de source d'événement Lambda.	25 novembre 2019

États des fonctions	Lorsque vous créez ou mettez à jour une fonction, celle-ci passe en état d'attente pendant que Lambda approvisionne les ressources pour sa prise en charge. Si vous connectez votre fonction à un VPC, Lambda peut créer immédiatement une interface réseau Elastic partagée, au lieu de créer des interfaces réseau lors de l'invocation de votre fonction. Cela se traduit par de meilleures performances pour VPC-connected les fonctions, mais peut nécessiter une mise à jour de votre automatisation. Pour plus d'informations, consultez États de fonction AWS Lambda.	25 novembre 2019
Options de gestion des erreurs pour les invocations asynchrones	De nouvelles options de configuration sont disponibles pour l'invocation asynchrone. Vous pouvez configurer Lambda de manière à limiter les nouvelles tentatives et à définir un âge d'événement maximal. Pour plus de détails, consultez Configuration de la gestion des erreurs pour les invocations asynchrones.	25 novembre 2019

Gestion des erreurs pour les sources d'événement de flux	De nouvelles options de configuration sont disponibles pour les mappages de source d'événement qui lisent depuis les flux. Vous pouvez configurer des mappages de source d'événements DynamoDB Streams et Kinesis Streams pour limiter les nouvelles tentatives et définir une ancienneté de registre maximale. Lorsque des erreurs se produisent, vous pouvez configurer le mappage de source d'événement pour fractionner les lots avant d'effectuer des nouvelles tentatives et d'envoyer des enregistrements d'invocations pour les lots ayant échoué vers une file d'attente ou une rubrique. Pour en savoir plus, consultez Mappage de source d'événement Lambda.	25 novembre 2019

Destinations pour les invocations asynchrones	Vous pouvez désormais configurer Lambda pour envoyer des enregistrements d'invocations asynchrones à un autre service. Les enregistrements d'invocation contiennent des détails sur l'événement, le contexte et la réponse de la fonction. Vous pouvez envoyer des enregistrements d'invocation à une file d'attente SQS, à une rubrique SNS, à une fonction Lambda ou à un bus d'événements. EventBridge Pour plus de détails, consultez Configuration des destinations pour les invocations asynchrones.	25 novembre 2019
Nouveaux environnements d'exécution pour Node.js Python et Java	De nouveaux environnements d'exécution sont disponibles pour Node.js 12, Python 3.8 et Java 11. Pour en savoir plus, consultez Environnements d'exécution Lambda.	18 novembre 2019
Prise en charge des files d'attente FIFO pour les sources d'événement Amazon SQS	Vous pouvez désormais créer un mappage de source d'événement qui lit à partir d'une file d'attente FIFO (premier entré, premier sorti). Auparavant, seules les files d'attente standard étaient prises en charge. Pour plus de détails, consultez Utilisation de Lambda avec Amazon SQS.	18 novembre 2019

Créer des applications dans la console Lambda	La création d'applications dans la console Lambda est désormais généralement disponible. Pour obtenir des instructions, consultez Managing applications in the Lambda console.	31 octobre 2019
Créer des applications dans la console Lambda (bêta)	Vous pouvez désormais créer une application Lambda avec un pipeline de livraison continue intégré dans la console Lambda. La console fournit des exemples d'applications que vous pouvez utiliser comme point de départ pour votre propre projet. Choisissez entre AWS CodeCommit et GitHub pour le contrôle de la source. Chaque fois que vous transmettez des modifications à votre référentiel, le pipeline inclus les construit et les déploie automatiquement. Pour obtenir des instructions, consultez Managing applications in the Lambda console.	3 octobre 2019

Améliorations des performances des VPC-connected fonctions	Lambda utilise désormais un nouveau type d'interface réseau Elastic qui est partagé par toutes les fonctions dans un sous-réseau Virtual Private Cloud (VPC). Lorsque vous connectez une fonction à un VPC, Lambda crée une interface réseau pour chaque combinaison de groupe de sécurité et de sous-rése au que vous choisissez. Lorsque les interfaces réseau partagées sont disponibles, la fonction n'a plus besoin de créer d'interfaces réseau supplémentaires au fur et à mesure de sa mise à l'échelle ascendante. Ainsi, les temps de démarrage sont considéra blement améliorés. Pour plus d'informations, consultez Configuration d'une fonction Lambda pour accéder aux ressources d'un VPC.	3 septembre 2019

Paramètres dpour les lots de flux	Vous pouvez désormais configurer une fenêtre de traitement par lots pour les mappages de source d'événements Amazon DynamoDB et Amazon Kinesis. Configurez une fenêtre de traitement par lots de cinq minutes maximum pour mettre en mémoire tampon les enregistrements entrants jusqu'à ce qu'un lot complet soit disponible. Cela réduit le nombre de fois où votre fonction est invoquée lorsque le flux est moins actif.	29 août 2019
CloudWatch Intégration de Logs Insights	La page de surveillance de la console Lambda inclut désormais des rapports provenant d'Amazon CloudWatch Logs Insights.	18 juin 2019
Amazon Linux 2018.03	L'environnement d'exécution Lambda est en cours de mise à jour pour utiliser Amazon Linux 2018.03. Pour plus de détails, consultez Environnement d'exécution.	21 mai 2019

Node.js 10	Un nouveau runtime est disponible pour Node.js 10, nodejs10.x. Ce runtime utilise la Node.js version 10.15 et sera régulièrement mis à jour avec la dernière version intermédiaire de la version Node.js 10. Node.js 10 est également le premier environnement d'exécution à utiliser Amazon Linux 2. Pour plus de détails, consultez Création de fonctions Lambda avec Node.js.	13 mai 2019
GetLayerVersionByArn API	Utilisez l'GetLayerVersionByArnAPI pour télécharger les informations de version de la couche avec l'ARN de version en entrée. Par rapport à GetLayerVersion, vous GetLayerVersionByArn permet d'utiliser l'ARN directement au lieu de l'analyser pour obtenir le nom de la couche et le numéro de version.	25 avril 2019
Ruby	AWS Lambda supporte désormais Ruby 2.5 avec un nouveau runtime. Pour plus d'informations, consultez Création de fonctions Lambda avec Ruby.	29 novembre 2018

Couches	Avec les couches Lambda, vous pouvez regrouper et déployer des bibliothèques, des environnements d'exécution personnalisés, ainsi que d'autres dépendances séparément depuis le code de votre fonction. Partagez vos couches avec vos autres comptes ou avec le monde entier. Pour plus de détails, consultez Couches Lambda.	29 novembre 2018
Exécutions personnalisées	Créez un environnement d'exécution (runtime) personnalisé pour exécuter des fonctions Lambda dans votre langage de programmation favori. Pour plus de détails, consultez Runtimes Lambda personnalisés.	29 novembre 2018
Déclencheurs d'Application Load Balancer	Elastic Load Balancing prend désormais en charge les fonctions Lambda en tant que cibles pour les équilibreurs de charge d'applications. Pour plus de détails, consultez Utilisation de Lambda avec des équilibreurs de charge des applications.	29 novembre 2018

Utiliser les consommateurs de Kinesis HTTP/2 Stream comme déclencheur	Vous pouvez utiliser les consommateurs de flux de HTTP/2 données Kinesis pour envoyer des événement s à AWS Lambda. Les consommateurs de flux disposent d'un débit de lecture dédié pour chaque fragment de votre flux de données et l'utilisent HTTP/2 pour minimiser la latence. Pour plus de détails, consultez Utilisation de Lambda avec Kinesis.	19 novembre 2018
Python 3.7	AWS Lambda supporte désormais Python 3.7 avec un nouveau runtime. Pour plus d'informations, consultez Création de fonctions Lambda avec Python.	19 novembre 2018
Augmentation de la limite de la charge utile d'invocation de fonction asynchrone	La taille maximum de charge utile pour les invocations asynchrones a augmenté de 128 Ko à 256 Ko, et correspon d à la taille maximum de message émis par un déclencheur Amazon SNS. Pour plus de détails, consultez Quotas Lambda.	16 novembre 2018
AWS GovCloud (US-East) Région	AWS Lambda est désormais disponible dans la région AWS GovCloud (US-East).	12 novembre 2018

AWS SAM Rubriques déplacées vers un guide du développeur distinct	Un certain nombre de sujets ont été axés sur la création d'applications sans serveur à l'aide du AWS Serverless Application Model (AWS SAM). Ces rubriques ont été déplacées vers le Guide du développeur AWS Serverless Application Model.	25 octobre 2018
Afficher des applications Lambda dans la console	Vous pouvez afficher l'état de vos applications Lambda sur la page Applications dans la console Lambda. Cette page indique l'état de la CloudFormation pile. Elle inclut des liens vers les pages où vous pouvez consulter plus d'informations sur les ressources figurant dans la pile. Vous pouvez également consulter les métriques agrégées pour l'application et créer des tableaux de bord de surveillance personnalisés.	11 octobre 2018
Délai d'attente d'exécution de la fonction	Pour permettre d'utiliser des fonctions de longue durée, le délai d'exécution maximal configurable est passé de 5 minutes à 15 minutes. Pour plus de détails, consultez Limites Lambda.	10 octobre 2018

Prise en charge PowerShell du langage de base dans AWS Lambda	AWS Lambda prend désormais en charge le langage PowerShell Core. Pour plus d'informations, voir Modèle de programmation pour la création de fonctions Lambda dans. PowerShell	11 septembre 2018
Prise en charge de l'exécution de .NET Core 2.1.0 dans AWS Lambda	AWS Lambda prend désormais en charge le runtime .NET Core 2.1.0. Pour en savoir plus, veuillez consulter la page .NET Core CLI.	9 juillet 2018
Mises à jour disponibles sur RSS	Vous pouvez maintenant vous abonner à un flux RSS pour suivre les versions de ce guide.	5 juillet 2018
Prise en charge d'Amazon SQS en tant que source d'événements	AWS Lambda prend désormais en charge Amazon Simple Queue Service (Amazon SQS) en tant que source d'événements. Pour plus d'informations, consultez Invocation des fonctions Lambda.	28 juin 2018

Région Chine (Ningxia)	AWS Lambda est désormais disponible dans la région Chine (Ningxia). Pour plus d'informations sur les régions et les points de terminaison Lambda, consultez Régions et points de terminaison (français non garanti) dans la Références générales AWS.	28 juin 2018

Mises à jour antérieures

Le tableau ci-après décrit les modifications importantes apportées dans chaque version du Manuel du développeur AWS Lambda avant juin 2018.

Modification	Description	Date
Support d'exécution pour Node.js Runtime 8.10	AWS Lambda prend désormais en charge la version Node.js d'exécution 8.10. Pour de plus amples informations, veuillez consulter Création de fonctions événementielles Lambda avec Node.js.	2 avril 2018
ID de révision des fonctions et alias	AWS Lambda prend désormais en charge les ID de révision sur les versions et alias de vos fonctions. Vous pouvez utiliser ces identifiants pour suivre et appliquer des mises à jour conditionnelles lorsque vous mettez à jour votre version de fonction ou vos ressources d'alias.	25 janvier 2018
Prise en charge de l'environnement d'exécution Go et .NET 2.0	AWS Lambda a ajouté la prise en charge de l'exécution pour Go et .NET 2.0. Pour plus d'informations, consultez Création de fonctions événementielles Lambda avec Go et Création de fonctions d'événement Lambda avec C#.	15 janvier 2018
Nouvelle conception de la console	AWS Lambda a introduit une nouvelle console Lambda pour simplifier votre expérience et a ajouté un éditeur de	30 novembre 2017

Modification	Description	Date
	code Cloud9 pour améliorer votre capacité à déboguer et à réviser le code de votre fonction.	
Définition de limites de simultanéité pour des fonctions individuelles	AWS Lambda prend désormais en charge la définition de limites de simultanéité pour les fonctions individuelles. Pour de plus amples informations, veuillez consulter Configuration de la simultanéité réservée pour une fonction événementielle.	30 novembre 2017
Déplacement du trafic avec des alias	AWS Lambda prend désormais en charge le transfert de trafic avec des alias. Pour de plus amples informations, veuillez consulter Création d'un déploiement continu avec des alias pondérés.	28 novembre 2017
Déploiement de code graduel	AWS Lambda permet désormais de déployer en toute sécurité de nouvelles versions de votre fonction Lambda à l'aide de Code Deploy. Pour plus d'informations, consultez Déploiement de code graduel.	28 novembre 2017
Région Chine (Pékin)	AWS Lambda est désormais disponible dans la région Chine (Pékin). Pour plus d'informations sur les régions et les points de terminaison Lambda, consultez Régions et points de terminaison (français non garanti) dans la Références générales AWS.	9 novembre 2017
Présentation de SAM Local	AWS Lambda présente SAM Local (désormais connu sous le nom de SAM CLI), un AWS CLI outil qui fournit un environnement vous permettant de développer, de tester et d'analyser vos applications sans serveur localement avant de les télécharger dans le runtime Lambda. Pour plus d'informations, consultez Test et débogage d'applications sans serveur.	11 août 2017

Modification	Description	Date
Canada (Central) Region	AWS Lambda est désormais disponible dans la région du Canada (Centre). Pour plus d'informations sur les régions et les points de terminaison Lambda, consultez Régions et points de terminaison (français non garanti) dans la Références générales AWS.	22 juin 2017
South America (São Paulo) Region	AWS Lambda est désormais disponible dans la région Amérique du Sud (São Paulo). Pour plus d'informations sur les régions et les points de terminaison Lambda, consultez Régions et points de terminaison (français non garanti) dans la Références générales AWS.	6 juin 2017
AWS Lambda support pour AWS X-Ray.	Lambda introduit la prise en charge de X-Ray, qui vous permet de détecter, d'analyser et d'optimiser les problèmes de performances de vos applications Lambda. Pour de plus amples informations, veuillez consulter Visualisez les invocations de la fonction d'événement Lambda à l'aide de AWS X-Ray.	19 avril 2017
Asia Pacific (Mumbai) Region	AWS Lambda est désormais disponible dans la région Asie-Pacifique (Mumbai). Pour plus d'informations sur les régions et les points de terminaison Lambda, consultez Régions et points de terminaison (français non garanti) dans la Références générales AWS.	28 mars 2017
AWS Lambda prend désormais en charge le Node.js runtime v6.10	AWS Lambda ajout du support pour le Node.js runtime v6.10. Pour de plus amples informations, veuillez consulter Création de fonctions événementielles Lambda avec Node.js.	22 mars 2017
Europe (London) Region	AWS Lambda est désormais disponible dans la région Europe (Londres). Pour plus d'informations sur les régions et les points de terminaison Lambda, consultez Régions et points de terminaison (français non garanti) dans la Références générales AWS.	1 février 2017

Modification	Description	Date
AWS Lambda prise en charge de l'environnement d'exécution .NET, de Lambda @Edge (version préliminaire), de Dead Letter Queues et du déploiement automatique d'applications sans serveur.	AWS Lambda ajout du support pour C#. Pour de plus amples informations, veuillez consulter Création de fonctions d'événement Lambda avec C#. Lambda @Edge vous permet d'exécuter des fonctions Lambda sur les emplacements AWS Edge en réponse à CloudFront des événements. Pour plus d'informations, consultez Customize at the edge with Lambda@Edge.	3 décembre 2016
AWS Lambda ajoute Amazon Lex en tant que source d'événements prise en charge.	Avec Lambda et Amazon Lex, vous pouvez créer rapidement des chatbots pour divers services, comme Slack et Facebook.	30 novembre 2016
US West (N. California) Region	AWS Lambda est désormais disponible dans la région Ouest des États-Unis (Californie du Nord). Pour plus d'informations sur les régions et les points de terminaison Lambda, consultez Régions et points de terminaison (français non garanti) dans la Références générales AWS.	21 novembre 2016

Modification	Description	Date
Présentation de la procédure AWS SAM de création et de déploiement d' Lambda-based applications et d'utilisation de variables d'environnement pour les paramètres de configuration de la fonction Lambda.	AWS SAM: Vous pouvez désormais utiliser le AWS SAM pour définir la syntaxe d'expression des ressources dans une application sans serveur. Pour déployer votre application, il vous suffit de spécifier les ressources dont vous avez besoin dans le cadre de votre application, ainsi que les politiques d'autorisations associées dans un fichier AWS CloudFormation modèle (écrit en JSON ou YAML), de regrouper vos artefacts de déploiement et de déployer le modèle. Variables d'environnement : vous pouvez utiliser des variables d'environnement afin de spécifier des paramètres de configuration pour votre fonction Lambda en dehors du code de votre fonction. Pour plus d'informations, consultez Utilisation des variables d'environnement Lambda.	18 novembre 2016
Asia Pacific (Seoul) Region	AWS Lambda est désormais disponible dans la région Asie-Pacifique (Séoul). Pour plus d'informations sur les régions et les points de terminaison Lambda, consultez Régions et points de terminaison (français non garanti) dans la Références générales AWS.	29 août 2016
Asia Pacific (Sydney) Region	Lambda est désormais disponible dans la région Asie-Pacifique (Sydney). Pour plus d'informations sur les régions et les points de terminaison Lambda, consultez Régions et points de terminaison (français non garanti) dans la Références générales AWS.	23 juin 2016
Mises à jour de la console Lambda	La console Lambda a été mise à jour pour simplifier le processus de création de rôles.	23 juin 2016
AWS Lambda prend désormais en charge le Node.js runtime v4.3	AWS Lambda ajout du support pour Node.js Runtime v4.3. Pour de plus amples informations, veuillez consulter Création de fonctions événementielles Lambda avec Node.js.	07 avril 2016

Modification	Description	Date
Région Europe (Frankfurt)	Lambda est désormais disponible dans la région Europe (Frankfurt). Pour plus d'informations sur les régions et les points de terminaison Lambda, consultez Régions et points de terminaison (français non garanti) dans la Références générales AWS.	14 mars 2016
Prise en charge de VPC	Vous pouvez maintenant configurer une fonction Lambda pour accéder aux ressources de votre VPC. Pour plus d'informations, consultez Permettre à Lambda Event Functions d'accéder aux ressources d'un Amazon VPC.	11 février 2016
Le runtime Lambda a été mis à jour.	L'environnement d'exécution a été mis à jour.	4 novembre 2015

Modification	Description	Date
Prise en charge de la gestion des versions, Python pour le développement de code pour des fonctions Lambda, événements planifiés et allongement du temps d'exécution	Vous pouvez désormais développer le code de la fonction Lambda à l'aide du langage Python. Pour plus d'informations, consultez Création de fonctions d'événement Lambda avec Python. Gestion des versions : vous pouvez conserver une ou plusieurs versions de la fonction Lambda. La gestion des versions vous permet de contrôler quelle version de fonction Lambda est exécutée dans des environnements différents (par exemple, développement, test ou production). Pour plus d'informations, consultez Gérer les versions de la fonction d'événement Lambda. Événements planifiés : vous pouvez également configurer Lambda pour invoquer régulièrement le code à l'aide de la console Lambda. Vous pouvez spécifier un taux fixe (nombre d'heures, de jours ou de semaines) ou vous pouvez spécifier une expression cron. Pour de plus amples informations, veuillez consulter Invoquer une fonction d'événement Lambda selon un calendrier. Rallongement du temps d'exécution : vous pouvez maintenant définir un temps d'exécution pouvant allant jusqu'à cinq minutes pour les fonctions Lambda afin de rendre possibles les fonctions de plus longue durée, telles que l'ingestion de données volumineuses et le traitement des tâches.	08 octobre 2015

Modification	Description	Date
Prise en charge de DynamoDB Streams	DynamoDB Streams est désormais disponible dans toutes les régions qui acceptent DynamoDB. Vous pouvez activer DynamoDB Streams pour votre table et utiliser une fonction Lambda comme déclencheur de cette table. Les déclencheurs sont des actions personnalisées que vous effectuez en réponse aux mises à jour apportées à la table DynamoDB. Pour afficher un exemple de procédure, veuillez consulter Tutoriel : Utilisation AWS Lambda avec les flux Amazon DynamoDB .	14 juillet 2015
Lambda prend désormais en charge l'appel de fonctions Lambda avec les clients. REST-compatible	Jusqu'à présent, pour invoquer votre fonction Lambda depuis votre application Web, mobile ou IoT, vous aviez besoin AWS des SDK (par exemple, AWS SDK pour Java, SDK pour Android ou AWS AWS SDK pour iOS). Lambda permet désormais d'invoquer une fonction Lambda auprès des REST-compatible clients via une API personnalisée que vous pouvez créer à l'aide d'Amazon API Gateway. Vous pouvez envoyer les requêtes à l'URL du point de terminaison de la fonction Lambda. Vous pouvez configurer la sécurité sur le terminal pour autoriser le libre accès, utiliser Gestion des identités et des accès AWS (IAM) pour autoriser l'accès ou utiliser des clés API pour contrôler l'accès à vos fonctions Lambda par d'autres personnes. Pour voir un exemple d'exercice de mise en route, veuillez consulter Invocation d'une fonction d'événement Lambda à l'aide d'un point de terminaison Amazon API Gateway.	09 juillet 2015
La console Lambda fournit maintenant des plans pour créer facilement des fonctions Lambda et les tester.	La console Lambda fournit un ensemble de plans. Chaque plan fournit un exemple de configuration de source d'événements et un exemple de code pour votre fonction Lambda, que vous pouvez utiliser pour créer facilement des Lambda-based applications. Tous les exercices de mise en route Lambda utilisent désormais les plans.	09 juillet 2015

Modification	Description	Date
Lambda prend désormais en charge Java pour créer vos fonctions Lambda.	Vous pouvez désormais créer le code Lambda en Java. Pour plus d'informations, consultez Création de fonctions d'événement Lambda avec Java.	15 juin 2015
Lambda prend désormais en charge la spécification d'un objet Amazon S3 en tant que fonction .zip lorsque vous créez ou mettez à jour une fonction Lambda.	Vous pouvez importer un package de déploiement de fonctions Lambda (fichier .zip) dans un compartiment Amazon S3 de la région dans laquelle vous souhaitez créer une fonction Lambda. Vous pouvez ensuite spécifier le nom du compartiment et le nom de la clé objet lorsque vous créez ou mettez à jour une fonction Lambda.	28 mai 2015
Lambda est désormais disponible de manière globale et prend en charge les backends mobiles	Lambda est désormais disponible de manière globale en production. Cette version présente également de nouvelles fonctionnalités qui facilitent la création de backends pour les mobiles, les tablettes et l'Internet des objets (IoT) via Lambda, qui adaptent automatiquement leur échelle, sans que vous ayez à mettre en service ou à gérer une infrastructure. Lambda prend désormais en charge les événements en temps réel (synchrones) et asynchrones. Les fonctionnalités supplémentaires comprennent la rationalisation de la configuration et de la gestion des sources d'événement. Le modèle d'autorisation et le modèle de programmation ont été simplifiés par la mise en place de stratégies de ressources pour les fonctions Lambda.	9 avril 2015
Version préliminaire	Version préliminaire du Guide du développeur AWS Lambda .	13 novembre 2014

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.